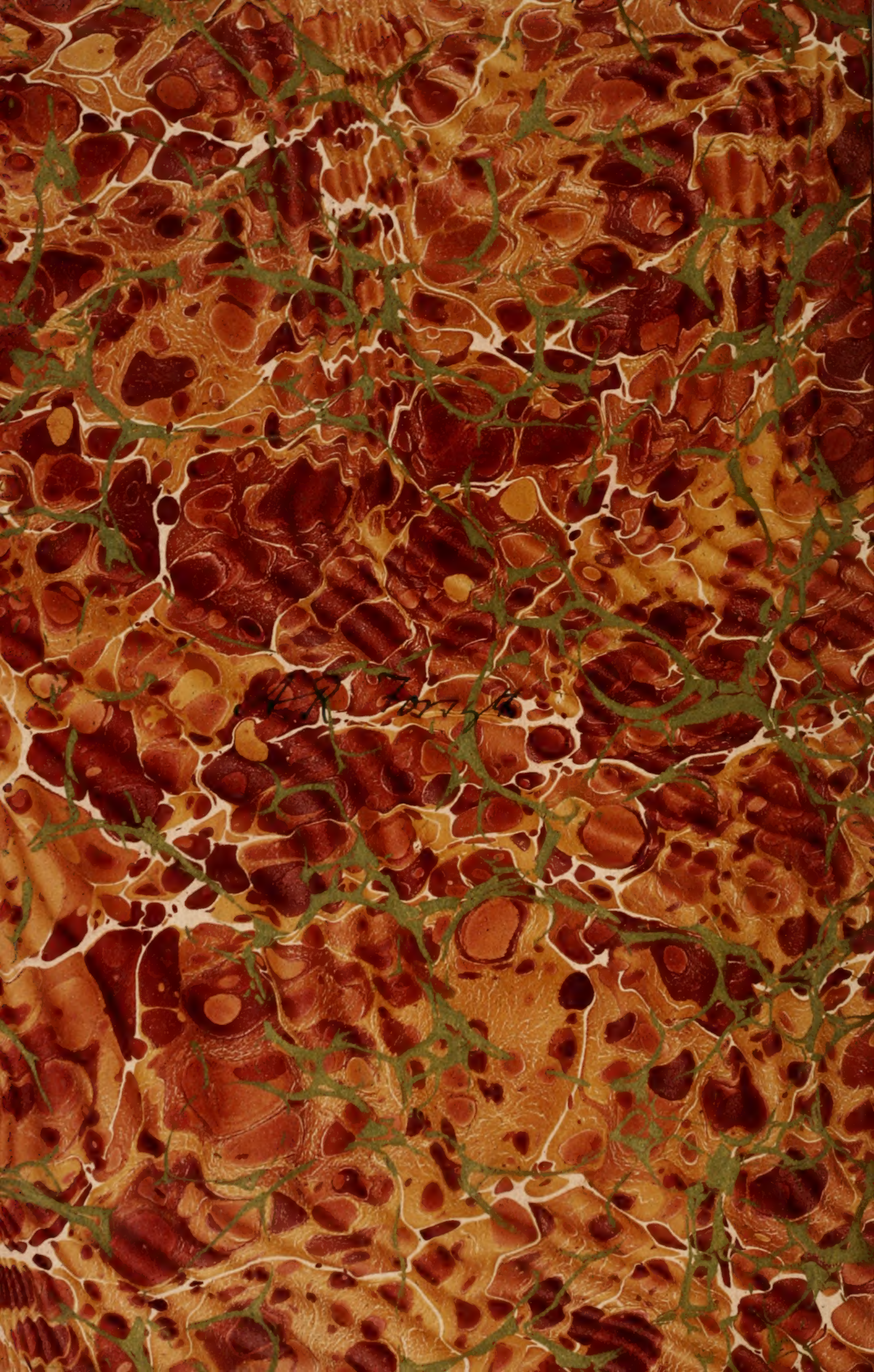
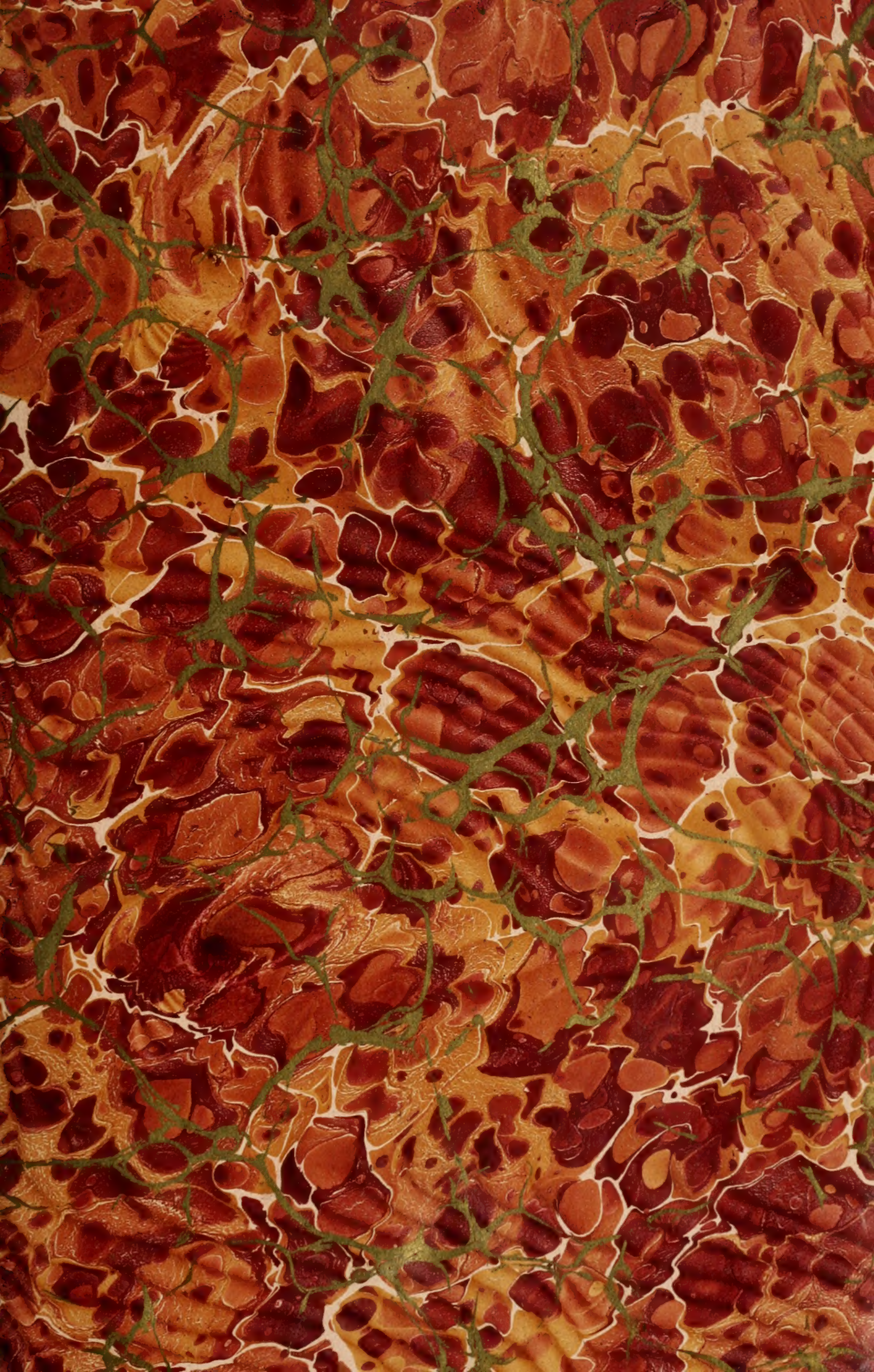






A.R. Forsyth





ELEMENTE

DER

ZAHLENTHEORIE

VON

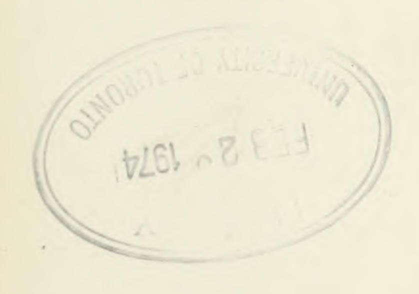
GUSTAV WERTHEIM.



LEIPZIG,

DRUCK UND VERLAG VON B. G. TEUBNER.

1887.



Vorwort.

Dieses Buch hat den Zweck, das Wichtigste aus den Elementen der Zahlentheorie in einfacher und übersichtlicher Darstellung zu geben. Es werden darin die Theilbarkeit der Zahlen, die Congruenzen ersten Grades, die Potenzreste und im Zusammenhang damit die binomischen Congruenzen, ferner die quadratischen Reste und die Congruenz zweiten Grades, endlich die binären quadratischen Formen, soweit die ganzzahlige Auflösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten es erfordert, eingehend behandelt. Da das Buch für Anfänger bestimmt ist und wohl nur an wenigen höheren Lehranstalten Zeit für eine gründliche Beschäftigung mit den in der Zahlentheorie vielfach angewandten Kettenbrüchen bleibt, so schien es mir rathsam, diesem Gegenstande ein besonderes Kapitel zu widmen.

Was die Darstellung betrifft, so habe ich besonderes Gewicht darauf gelegt, die wichtigeren Sätze und Verfahrungsarten durch Beispiele und durch mehr oder weniger vollständig gelöste Aufgaben, die zum Theil den trefflichen Sammlungen von Heis, Bardey und Meier Hirsch entnommen sind, zu befestigen. Durch diese wiederholte Anwendung hoffe ich den Lernenden in den wirklichen Besitz der vorgetragenen Lehren zu setzen und ihn zu einem genussreichen Studium der klassischen Werke und Arbeiten über Zahlentheorie zu befähigen und zu veranlassen.

Frankfurt a. M., im Februar 1887.

G. Wertheim.

Inhaltsverzeichniss.

Erstes Kapitel.

Theilbarkeit der Zahlen.

Zweites Kapitel.

Congruente Zahlen.

Drittes Kapitel.

Congruenzen ersten Grades.

Viertes Kapitel.

Kettenbrüche.

Fünftes Kapitel.

Potenzreste für Primzahlmoduln.

Sechstes Kapitel.

Potenzreste für zusammengesetzte Moduln.

Siebentes Kapitel.

Congruenzen zweiten Grades.

Achtes Kapitel.

Allgemeine Sätze über binäre quadratische Formen und die Darstellung der Zahlen durch dieselben.

Neuntes Kapitel.

Quadratische Formen mit negativer Determinante.

Zehntes Kapitel.

Quadratische Formen mit positiver nichtquadratischer Determinante.

Elftes Kapitel.

Formen, deren Determinante ein Quadrat oder gleich Null ist. Auflösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten.



Erstes Kapitel.

Theilbarkeit der Zahlen.

§ 1. Definition. — Jede Zahl a lässt sich durch sich selbst und durch die Einheit ohne Rest theilen, hat also wenigstens zwei Divisoren, nämlich a und 1. Eine Zahl, welche nur diese beiden Divisoren zulässt, wird eine absolute Primzahl oder schlechtweg eine Primzahl genannt. Eine Zahl, die dieser Definition nicht entspricht, heisst zusammengesetzt.

Eine Primzahl ist z. B. 13; dagegen ist die Zahl 15 zusammengesetzt, da sie ausser 1 und 15 auch noch die Divisoren 3 und 5 hat.

§ 2. Ermittlung der Primzahlen. — Die einzige gerade Primzahl ist 2; alle übrigen Primzahlen sind ungerade. Daher hat man, um die Primzahlen zu ermitteln, nur die ungeraden Zahlen

$$3, 5, 7, 9, 11, 13, 15, 17, \ldots$$

ins Auge zu fassen. Aus dieser Reihe scheidet man nach einem dem Eratosthenes (250 v. Chr.) zugeschriebenen Verfahren („Sieb des Eratosthenes") die zusammengesetzten Zahlen in folgender Weise aus:

Man streicht, mit 3 beginnend, die 3te Zahl, d. i. 9, die 6te, d. i. 15, die 9te, 12te, u. s. w. Zahl aus; dadurch fallen aus der Reihe der ungeraden Zahlen offenbar die durch 3 theilbaren Zahlen 9, 15, 21, 27, . . . weg. Weiter streicht man, mit 5 beginnend, die 5te, 10te, 15te, . . . Zahl aus, wobei die bereits weggefallenen Zahlen mitzuzählen sind, und entfernt dadurch alle durch 5 theilbaren ungeraden Zahlen 15, 25, ... Ebenso verfährt man weiter mit 7, 11, 13, ... Die nach

dieser Operation stehen gebliebenen Zahlen sind die sämmtlichen in dem betrachteten Gebiet vorhandenen Primzahlen.

Es fragt sich nun, welches die letzte Primzahl ist, mit der man diese Abzählung beginnen muss, um alle Primzahlen bis zu einer gewissen Grenze a zu erhalten. Das ergiebt sich aus folgender Bemerkung: Wenn eine zwischen 1 und a liegende Zahl b das Produkt zweier Faktoren m, n ist ($b = m \,.\, n$), von denen der eine mehr als $\sqrt{a}$ beträgt, so muss der andere $< \sqrt{a}$ sein. Die Zahl b fällt demnach bei dem obigen Verfahren schon durch die mit dem kleineren Factor beginnende Abzählung weg, und es ist überflüssig, die Abzählung von dem grösseren Factor aus vorzunehmen. Die letzte Zahl, von der aus man abzuzählen hat, um alle zwischen 1 und a liegenden Primzahlen zu finden, ist also die grösste Primzahl welche kleiner oder gleich $\sqrt{a}$ ist.

Beispiel. Da $\sqrt{100} = 10$ und 7 die grösste Primzahl unter 10 ist, so hat man, um alle Primzahlen bis 100 zu erhalten, in der oben dargelegten Weise nur mit den Zahlen 3, 5, 7 zu verfahren. Man erhält, wenn die wegfallenden Zahlen in Klammern gesetzt werden,

3, 5, 7, [9], 11, 13, [15], 17, 19, [21], 23, [25], [27], 29, 31, [33], [35], 37, [39], 41, 43, [45], 47, [49], [51], 53, [55], [57], 59, 61, [63], [65], 67, [69], 71, 73, [75], [77], 79, [81], 83, [85], [87], 89, [91], [93], [95], 97, [99].

§ 3. Anzahl der Primzahlen. — **Lehrsatz.** Die natürliche Zahlenreihe enthält unendlich viele Primzahlen (Euklid's Elemente, Buch IX, Satz 20).

Beweis. Wäre die Anzahl der Primzahlen eine endliche und p die grösste derselben, so könnten wir alle vorhandenen Primzahlen 2, 3, 5, ..., p mit einander multipliciren und das Produkt um eine Einheit vergrössern. Die erhaltene Zahl

$$A = 2 \,.\, 3 \,.\, 5 \ldots p + 1$$

wäre nun jedenfalls grösser als p und durch keine der vorhandenen Primzahlen 2, 3, ..., p theilbar, da sie ja für jede derselben den Rest 1 liefert. A müsste also entweder selbst eine Primzahl oder durch über p hinausliegende Primzahlen theilbar sein.

In jedem Falle existirt also, im Widerspruch mit unserer Annahme, eine Primzahl, die grösser als p ist, und die Reihe der Primzahlen ist daher, wie die natürliche Zahlenreihe selbst, unbegrenzt.

Anmerkung. Der vorstehende Satz ist ein specieller Fall des allgemeineren, von Lejeune Dirichlet in den Abhandlungen der Berliner Akademie 1837 bewiesenen Satzes: Jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, enthält unendlich viele Primzahlen.

§ 4. Zusammengesetzte Zahlen und Zerlegung derselben. — Eine zusammengesetzte Zahl m lässt sich der Definition nach als das Produkt zweier Factoren darstellen, von denen jeder kleiner als m ist. Jeder dieser Factoren ist entweder eine Primzahl oder zusammengesetzt. Im letzteren Falle lässt er sich wieder in zwei Factoren zerlegen, von denen jeder kleiner als er selbst ist. Da man auf diese Weise zu immer kleineren Factoren gelangt, und es nicht unendlich viele ganze Zahlen geben kann, die kleiner als m sind, so muss man endlich zu Zahlen gelangen, die nicht weiter zerlegt werden können, d. h. zu Primzahlen. Jede zusammengesetzte Zahl kann also als das Produkt von Primzahlen dargestellt werden. Es ist z. B. $60 = 2 \,.\, 2 \,.\, 3 \,.\, 5$.

Tritt in der Zerlegung einer Zahl m eine Primzahl a wiederholt, etwa αmal, als Factor auf, so schreibt man statt der α Factoren a einfach die Potenz a^α. Ebenso verfährt man mit den übrigen Primzahlfactoren $b, c, \ldots$, die beziehungsweise β, $\gamma, \ldots$ mal vorhanden sein mögen. Dann wird die Zahl m auf die Form

$$m = a^\alpha \, b^\beta \, c^\gamma \ldots$$

gebracht, wo $a, b, c, \ldots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \ldots$ ganze positive Zahlen bezeichnen. Beispiel: $504 = 2^3 \,.\, 3^2 \,.\, 7$.

Es lässt sich nun zeigen, dass jede zusammengesetzte Zahl nur auf eine Weise in Primzahlfactoren zerlegt werden kann. Der Beweis wird geführt mittels der beiden folgenden Hilfssätze:

Hilfssatz I. Das Produkt zweier ganzen Zahlen, die kleiner als eine Primzahl p sind, ist durch p nicht theilbar.

Beweis. Wir nehmen an, es gebe zwischen 1 und p mehrere Zahlen $b, c, d, \ldots$ von der Beschaffenheit, dass das Produkt einer jeden in die demselben Intervall angehörende Zahl a durch p theilbar sei. Die kleinste dieser Zahlen $b, c, d, \ldots$ sei b. Nun muss erstens $b > 1$ sein; denn für $b = 1$ wäre $ab = a$, also a, der Voraussetzung zuwider, durch p theilbar. Ferner kann b nicht in p aufgehen, da p eine Primzahl ist. Wir werden also, wenn wir p durch b dividiren, einen Quotienten q und einen Rest r erhalten, welcher letzterer von Null verschieden und kleiner als b ist. Es ist dann

$$p = bq + r,$$

folglich

$$ap = abq + ar.$$

Nun ist offenbar aber ap und (der Voraussetzung nach) auch abq durch p theilbar; p muss daher auch in ar aufgehen, d. h. r muss sich unter den Zahlen $b, c, d, \ldots$ vorfinden. Unsere Annahme, b sei die kleinste dieser Zahlen, führt also zu dem Resultat, dass es eine noch kleinere Zahl r von derselben Beschaffenheit gebe. Es giebt also überhaupt keine Zahl zwischen 1 und p, deren Produkt in a durch p theilbar wäre.

Hilfssatz II. Wenn weder a noch b durch die Primzahl p theilbar ist, so ist auch das Produkt ab nicht durch p theilbar.

Beweis. Wir dividiren jede der beiden Zahlen a, b durch p und nennen die erhaltenen Quotienten A, B, die erhaltenen Reste α, β, so ist

$$a = Ap + \alpha, \quad b = Bp + \beta,$$

also

$$ab = (ABp + \alpha B + \beta A)p + \alpha\beta.$$

Wäre nun ab durch p theilbar, so müsste p offenbar auch in $\alpha\beta$ aufgehen. Das ist aber, da jede der Zahlen α, β kleiner als p ist, nach dem vorigen Satze unmöglich.

Zusatz. Wenn keine der Zahlen $a, b, c, d, \ldots$ durch die Primzahl p theilbar ist, so ist auch das Produkt $abcd \ldots$ durch p nicht theilbar.

Beweis. Nach dem Hilfssatz II ist ab nicht durch p theilbar; folglich geht p nach demselben Satze auch nicht in $ab \,.\, c = abc$ auf, u. s. w.

Lehrsatz. Eine jede zusammengesetzte Zahl kann nur auf **eine** Weise in Primzahlfactoren zerlegt werden.

Beweis. Angenommen, die Zahl

$$A = a^\alpha\, b^\beta\, c^\gamma \ldots,$$

wo $a, b, c, \ldots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \ldots$ ganze positive Zahlen sind, sei noch auf eine zweite Weise in Primzahlfactoren zerlegt worden. Dann kann das zweite Factoren-System keine Primzahl enthalten, die sich nicht auch im ersteren vorfindet; denn eine solche würde nach dem vorhergehenden Zusatz nicht in $a^\alpha b^\beta c^\gamma \ldots$, d. h. nicht in A aufgehen. Ebenso kann dem zweiten System keine Primzahl des ersten fehlen; denn eine solche würde nach demselben Zusatz nicht in das Produkt der Zahlen des zweiten Systems, d. h. nicht in A aufgehen.

Beide Systeme könnten sich also nur dadurch unterscheiden, dass ein und dieselbe Primzahl in dem einen System einen grösseren Exponenten als in dem anderen hätte. Es sei p eine solche Primzahl, welche in dem einen System den Exponenten m, im anderen System einen grösseren Exponenten $m + n$ habe. Dann würden sich für die Zahl $\frac{A}{p^m}$ zwei Zerlegungen ergeben, von denen die eine die Primzahl p gar nicht, die andere den Factor p^n enthielte, was, wie wir bereits gezeigt haben, unmöglich ist. Beide Zerlegungen stimmen also auch hinsichtlich der Exponenten vollständig überein.

§ 5. Divisoren einer Zahl. — Hat man eine Zahl m auf die Form

$$m = a^\alpha\, b^\beta\, c^\gamma \ldots$$

gebracht, wo $a, b, c, \ldots, \alpha, \beta, \gamma, \ldots$ die schon mehrfach angegebene Bedeutung haben, so ist es leicht, ihre sämmtlichen Divisoren zu bilden.

m hat zunächst des Factors a^α wegen die $\alpha + 1$ Divisoren

(I) $$1, a, a^2, \ldots, a^\alpha.$$

Weil ferner m auch den Factor b^β enthält, so geht weiter jede Zahl in m auf, die entsteht, wenn man die Zahlen (I) der Reihe nach mit jeder der Zahlen $b, b^2, \ldots, b^\beta$ multiplicirt. Man erhält auf diese Weise aus jeder der Zahlen (I) β, also im Ganzen $(\alpha + 1)\beta$ neue Divisoren von m, nämlich

$$\text{(II)}\qquad b,\ ab,\ a^2b,\ \ldots,\ a^\alpha b;\ b^2,\ ab^2,\ a^2b^2,\ \ldots,\ a^\alpha b^2;$$
$$\ldots;\ b^\beta,\ ab^\beta,\ a^2b^\beta,\ \ldots,\ a^\alpha b^\beta,$$

und die Gesammtzahl der Divisoren, die nur aus a und b gebildet sind, ist

$$(\alpha + 1) + (\alpha + 1)\beta = (\alpha + 1)(\beta + 1).$$

Dazu kommen weiter wegen des Factors c^γ alle Zahlen, die man erhält, wenn man die $(\alpha + 1)(\beta + 1)$ Zahlen (I) und (II) der Reihe nach mit $c, c^2, \ldots, c^\gamma$ multiplicirt. Dies liefert $(\alpha + 1)(\beta + 1)\gamma$ neue Divisoren. Man hat dann im Ganzen

$$(\alpha + 1)(\beta + 1) + (\alpha + 1)(\beta + 1)\gamma$$
$$= (\alpha + 1)(\beta + 1)(\gamma + 1)$$

Divisoren. Durch Fortsetzung dieser Schlüsse erkennt man, dass die Zahl

$$m = a^\alpha b^\beta c^\gamma \ldots k^\varkappa$$

genau

$$(\alpha + 1)(\beta + 1)(\gamma + 1)\ldots(\varkappa + 1)$$

Divisoren hat, die, wie man leicht sieht, die sämmtlichen Glieder des Produkts

$$(1 + a + a^2 + \cdots + a^\alpha)$$
$$\times (1 + b + b^2 + \cdots + b^\beta)\cdots(1 + k + \cdots + k^\varkappa)$$

sind, deren Summe also

$$\frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdots \frac{k^{\varkappa+1} - 1}{k - 1}$$

ist.

Beispiel. Die Zahl $504 = 2^3 \cdot 3^2 \cdot 7$ hat zu Divisoren die 24 Glieder des Produkts

$$(1 + 2 + 2^2 + 2^3)(1 + 3 + 3^2)(1 + 7);$$

diese sind, der Grösse nach geordnet, 1, 2, 3, 4, 6, 7. 8, 9, 12, 14, 18, 21, 24, 28, 36, 42, 56, 63, 72, 84, 126, 168, 252, 504 und haben zur Summe

$$\frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot 8 = 1560.$$

Anmerkung. Eine merkwürdige Formel zur Berechnung der Summe der Divisoren einer Zahl ist von Euler gefunden und nach vielen Bemühungen von demselben bewiesen worden. (Euler, Commentationes Algebr. Collectae, Petropoli 1849, T. I, p. 146 ff.).

Vollkommene Zahlen. — Eine Zahl, welche der Summe ihrer Divisoren, die Zahl selbst ausgeschlossen, gleich ist, heisst vollkommen.

Alle uns bekannten Zahlen dieser Art liefert der Satz von Euklid (Elemente, Buch IX, 36). Addirt man von der Einheit an so viele Glieder der geometrischen Progression 1, 2, 4, 8, ..., bis deren Summe eine Primzahl wird, so ist das Produkt aus dieser Summe und dem letzten Gliede, das genommen wurde, eine vollkommene Zahl.

Beweis. Es sei $s = 1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$ eine Primzahl, so ist zu zeigen, dass die Summe der Divisoren des Produkts $(2^n - 1)\, 2^{n-1}$ gleich diesem Produkt selbst sei. Diese Divisoren sind aber, da $2^n - 1$ eine Primzahl ist, die der Kürze wegen mit p bezeichnet werden möge,

$$1,\ 2,\ 2^2,\ \ldots,\ 2^{n-1},\ p,\ 2p,\ 2^2 p,\ \ldots,\ 2^{n-2} p,$$

haben also zur Summe

$$2^n - 1 + p\,(2^{n-1} - 1)$$
$$= 2^n - 1 + (2^n - 1)\,(2^{n-1} - 1) = (2^n - 1)\, 2^{n-1}.$$

Beispiele. Den Werthen $n = 2, 3, 5, 7$ entsprechen beziehungsweise die vollkommenen Zahlen 6, 28, 496, 8128.

Befreundete Zahlen. — Zwei Zahlen heissen befreundet, wenn jede derselben der Summe der Divisoren der anderen, die Zahl selbst ausgeschlossen, gleich ist. (Vergl. Euler, Opuscula, T. II. p. 23 ff). Von dieser Art sind z. B. die beiden Zahlen 220 und 284; denn die Divisoren von 220 haben die Summe

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284,$$

und die Divisoren von 284 haben die Summe

$$1 + 2 + 4 + 71 + 142 = 220.$$

§ 6. Der grösste gemeinschaftliche Divisor von Zahlen. — Wenn Zahlen in ihre Primzahlfactoren zerlegt sind, so bildet man ihren grössten gemeinschaftlichen Divisor auf folgende Weise: Man nimmt jede Primzahl, die allen gegebenen Zahlen gemeinschaftlich ist, giebt ihr den kleinsten Exponenten,

den sie in einer dieser Zahlen hat, und multiplicirt die so erhaltenen Potenzen.

Beispiel. Die Zahlen

$$504 = 2^3 . 3^2 . 7, \; 240 = 2^4 . 3 . 5 \text{ und } 864 = 2^5 . 3^3$$

haben als grössten gemeinschaftlichen Divisor $2^3 . 3 = 24$.

Wir werden jetzt zeigen, wie man verfährt, wenn die gegebenen Zahlen nicht in ihre Primzahlfactoren zerlegt sind und auch nicht erst zerlegt werden sollen.

Aufgabe I. Den grössten gemeinschaftlichen Divisor zweier Zahlen a und $b < a$ zu ermitteln.

1. Fall. Wenn die Zahl b in a aufgeht, so ist sie, da sie auch in sich selbst aufgeht, ein gemeinschaftlicher Divisor von a und b. Sie ist aber auch der grösste gemeinschaftliche Divisor, weil keine grössere Zahl als b in b aufgehen kann.

2. Fall. b geht nicht in a auf. Erhält man bei der Division einer beliebigen Zahl α durch eine Zahl β einen Quotienten $\varkappa$ und einen Rest $\varrho < \beta$, so ist $\alpha = \beta\varkappa + \varrho$, und man erkennt leicht, dass der grösste gemeinschaftliche Divisor von α und β mit dem grössten gemeinschaftlichen Divisor von β und ϱ übereinstimmt.

Dies vorausgesetzt, dividiren wir mit b in a, mit dem Rest r, der kleiner als b ist, in b, mit dem neuen Rest r_1, der kleiner als r sein wird, in r, u. s. w., und erhalten, da die Reste immer kleiner werden, also endlich einmal der Rest Null erscheinen muss, die Gleichungen

$$\begin{aligned}
a &= bq + r \\
b &= rq_1 + r_1 \\
r &= r_1 q_2 + r_2 \\
&\cdots\cdots\cdots \\
r_{m-1} &= r_m q_{m+1} + r_{m+1} \\
r_m &= r_{m+1} q_{m+2} .
\end{aligned}$$

Da nun die Zahlenpaare a und b, b und r, r und r_1, ..., r_{m-1} und r_m, r_m und r_{m+1} denselben grössten gemeinschaftlichen Divisor haben, und da r_{m+1} der grösste gemeinschaftliche Divisor des letzten Paares ist, so ist r_{m+1} auch der grösste gemeinschaftliche Divisor von a und b.

Aufgabe II. Den grössten gemeinschaftlichen Divisor mehrerer Zahlen $a, b, c, \ldots$ zu bestimmen.

Man ermittle zunächst den grössten gemeinschaftlichen Divisor d der beiden Zahlen a und b, und sodann den grössten gemeinschaftlichen Divisor d' von d und c, so ist d' der grösste gemeinschaftliche Divisor der drei Zahlen a, b, c; denn d' geht in c und, weil in d, auch in a und b auf, ist also ein Divisor von a, b, c. Hätten nun die drei Zahlen a, b, c einen gemeinschaftlichen Divisor δ, der grösser als d' wäre, so würde δ in c und, weil in a und b, auch in d aufgehen, d. h. c und d würden einen gemeinschaftlichen Divisor haben, der grösser als ihr grösster gemeinschaftlicher Divisor wäre. Es ist also in der That d' der grösste gemeinschaftliche Divisor von a, b, c.

Man sieht leicht, wie man durch wiederholte Anwendung dieses Verfahrens den grössten gemeinschaftlichen Divisor beliebig vieler Zahlen bestimmen kann.

§ 7. Relative Primzahlen. — Zwei Zahlen heissen prim zu einander oder relative Primzahlen, wenn ihr grösster gemeinschaftlicher Divisor die Einheit ist.

15 und 8 sind prim zu einander, 15 und 12 nicht.

Lehrsatz I. Wenn die Zahlen a und b prim zu einander sind, so geht jeder gemeinschaftliche Divisor von ak und b in k auf.

Beweis. Da a und b relative Primzahlen sind, so gelangt man bei den in § 6 Aufgabe I angegebenen Divisionen zu dem Rest 1, erhält also die Gleichungen

$$\begin{aligned} a &= bq + r \\ b &= rq_1 + r_1 \\ &\cdots\cdots\cdots \\ r_{m-1} &= r_m q_{m+1} + 1 . \end{aligned}$$

Werden dieselben sämmtlich mit k multiplicirt, so verwandeln sie sich in

$$\begin{aligned} ak &= bqk + rk \\ bk &= rq_1k + r_1k \\ &\cdots\cdots\cdots \\ r_{m-1}k &= r_m q_{m+1}k + k , \end{aligned}$$

und daraus erkennt man, dass ein gemeinschaftlicher Divisor

von ak und b auch in rk, folglich, weil in b und rk, auch in r_1k, u. s. w., endlich auch in k aufgehen muss.

Ist im Besonderen ak durch b theilbar, so muss k durch b theilbar sein.

Lehrsatz II. Wenn jede der beiden Zahlen a, k prim zu b ist, so ist auch das Produkt ak prim zu b.

Beweis. Ein gemeinschaftlicher Divisor von ak und b müsste, da a prim zu b ist, nach dem vorigen Satze in k aufgehen, während k prim zu b sein soll.

Zusatz. Potenzen relativer Primzahlen sind prim zu einander.

Beweis. Wenn a prim zu b ist, so ist nach dem vorigen Satze auch a^2, daher nach demselben Satze auch a^3, u. s. w., allgemein a^m prim zu b. Auf dieselbe Weise folgt aus der Annahme, b sei prim zu a^m, dass auch b^2, b^3, u. s. w., allgemein b^n prim zu a^m sein muss. a^m und b^n sind mithin relative Primzahlen.

§ 8. Das kleinste Vielfache von Zahlen. — Unter dem kleinsten Vielfachen der Zahlen $a, b, c, \ldots$ versteht man die kleinste Zahl, welche durch jede der Zahlen $a, b, c, \ldots$ theilbar ist.

Wenn die Zahlen $a, b, c, \ldots$ in ihre Primzahlfaktoren zerlegt sind, so bildet man das kleinste Vielfache derselben auf folgende Weise: Man nimmt jede Primzahl, die in einer der Zahlen $a, b, c, \ldots$ vorkommt, giebt ihr den grössten Exponenten, den sie in einer derselben hat, und bildet das Produkt aller so erhaltenen Potenzen.

Beispiel. Die Zahlen

$$504 = 2^3 . 3^2 . 7, \quad 240 = 2^4 . 3 . 5, \quad 864 = 2^5 . 3^3$$

haben das kleinste Vielfache

$$2^5 . 3^3 . 5 . 7 = 30240.$$

Wir wollen jetzt zeigen, wie man das kleinste Vielfache gegebener Zahlen ermittelt, ohne ihre Primzahlfactoren zu benutzen.

Aufgabe I. Das kleinste Vielfache zweier Zahlen a, b zu finden.

1. Fall. Wenn a und b prim zu einander sind, so ist das Produkt ab das kleinste Vielfache beider Zahlen.

Das kleinste Vielfache muss nämlich durch a theilbar, also von der Form ak sein, wo k eine ganze positive Zahl ist. ak soll aber auch durch b theilbar sein, und da a prim zu b ist, so erfordert dies nach § 7 Lehrsatz I, dass k durch b theilbar, also $k = bl$ sei, wo l eine ganze positive Zahl bezeichnet. Die durch a und zugleich durch b theilbaren Zahlen haben also die Form $ak = abl$ und werden erhalten, indem man l der Reihe nach die Werthe 1, 2, 3, ... beilegt. Die kleinste dieser Zahlen, d. i. das kleinste Vielfache von a und b entspricht dem Werthe $l = 1$ und ist ab.

2. Fall. Haben a und b einen grössten gemeinschaftlichen Divisor d, so ist

$$d \cdot \frac{a}{d} \cdot \frac{b}{d}$$

das kleinste Vielfache von a und b. Es sei nämlich

$$a = \alpha d, \quad b = \beta d,$$

wo α und β relative Primzahlen sind. Dann ist jedes Vielfache von a von der Form $\alpha d k$. Soll dasselbe durch $b = \beta d$ theilbar sein, so muss β in αk und, da β prim zu α ist, β in k aufgehen. k ist also von der Form βl, wo l eine ganze positive Zahl bezeichnet. Die Vielfachen von a und b sind daher in dem Ausdruck $\alpha\beta d l$ enthalten und ergeben sich, wenn man l der Reihe nach die Werthe 1, 2, 3, ... beilegt. Das kleinste Vielfache entspricht dem Werthe $l = 1$ und ist

$$\alpha\beta d = d \,.\, \alpha \,.\, \beta = d \cdot \frac{a}{d} \cdot \frac{b}{d} \cdot$$

Aufgabe II. Das kleinste Vielfache beliebig vieler gegebenen Zahlen $a, b, c, \ldots$ zu finden.

Auf die im Vorigen angegebene Weise lässt sich das kleinste Vielfache m der beiden Zahlen a und b und sodann das kleinste Vielfache m_1 von m und c bestimmen; m_1 ist dann, wie wir zeigen wollen, das kleinste Vielfache der drei Zahlen a, b, c.

Da die durch a und b theilbare Zahl m in m_1 aufgeht, so geht sowohl a als auch b in m_1 auf. m_1 ist aber auch ein Vielfaches von c, also ist m_1 ein Vielfaches der drei Zahlen a, b, c.

Es ist jetzt noch zu beweisen, dass m_1 das kleinste Vielfache von a, b, c ist. Gäbe es eine Zahl $\mu < m_1$, welche

durch a, b, c theilbar wäre, so müsste dieselbe, weil durch a und b, auch durch m, und, weil durch m und c, auch durch m_1 theilbar sein. Das ist aber unmöglich, da $\mu < m_1$ sein soll. m_1 ist somit in der That das kleinste Vielfache der drei Zahlen a, b, c.

Man sieht leicht, wie man durch wiederholte Anwendung dieses Verfahrens das kleinste Vielfache beliebig vieler Zahlen bestimmt.

§ 9. Die Function $\varphi(m)$. — Von besonderem Interesse ist es, zu bestimmen, wie viele Zahlen prim zu einer gegebenen Zahl m und nicht grösser als m sind. Die Anzahl dieser Zahlen pflegt man mit $\varphi(m)$ zu bezeichnen.

So giebt es eine Zahl, nämlich 1, welche prim zu 1 und nicht > 1 ist; es ist folglich $\varphi(1) = 1$.

Prim zu 6 und nicht grösser als 6 sind die beiden Zahlen 1 und 5; also ist $\varphi(6) = 2$. Ebenso erhält man leicht

$$\varphi(2) = 1\,, \quad \varphi(3) = 2\,, \quad \varphi(4) = 2\,, \quad \varphi(5) = 4\,,$$

u. s. w. Um allgemein $\varphi(m)$ zu bestimmen, denken wir uns m in seine Primzahlfactoren zerlegt,

$$m = a^\alpha b^\beta c^\gamma \ldots,$$

wo wieder a, b, c, ... ungleiche Primzahlen, α, β, γ, ... ganze positive Zahlen bezeichnen. Es handelt sich dann darum, aus der Reihe

$$\text{(I)} \qquad 1, 2, 3, \ldots, m$$

jede Zahl zu entfernen, welche durch eine oder mehrere der Primzahlen a, b, c, ... theilbar ist, und die stehen gebliebenen Zahlen zu zählen.

Durch a sind theilbar die $\frac{m}{a}$ Zahlen

$$a\,, 2a\,, 3a\,, \ldots, \frac{m}{a}\,a\,.$$

Streicht man diese Zahlen aus, so bleiben in der Reihe (I) noch

$$m - \frac{m}{a} = m\left(1 - \frac{1}{a}\right)$$

Zahlen stehen, von denen keine durch a theilbar ist.

Zweitens haben wir die Zahlen wegzulassen, welche den Factor b enthalten. Es sind dies die $\frac{m}{b}$ Zahlen

$$b,\ 2b,\ 3b, \ldots, \frac{m}{b} b.$$

Einige derselben sind aber schon weggefallen, weil sie auch durch a theilbar sind, nämlich die $\frac{m}{ab}$ Zahlen

$$ab,\ 2ab,\ 3ab, \ldots, \frac{m}{ab} ab.$$

Die Reihe (I) enthält also

$$\frac{m}{b} - \frac{m}{ab} = \frac{m}{b}\left(1 - \frac{1}{a}\right)$$

Zahlen, welche durch b, nicht aber auch durch a theilbar sind, folglich

$$m\left(1 - \frac{1}{a}\right) - \frac{m}{b}\left(1 - \frac{1}{a}\right) = m\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

Zahlen, welche weder den Factor a, noch den Factor b enthalten.

Drittens haben wir die $\frac{m}{c}$ durch c theilbaren Zahlen der Reihe (I)

$$\text{(II)} \qquad c,\ 2c,\ 3c, \ldots, \frac{m}{c} c$$

zu betrachten und zu bestimmen, wie viele derselben nicht schon fortgefallen sind, d. h. wie viele von ihnen weder a noch b als Factor enthalten. Da nun c als Primzahl nicht durch a oder b theilbar ist, so läuft diese Aufgabe darauf hinaus, zu untersuchen, wie viele Zahlen der Reihe

$$\text{(III)} \qquad 1,\ 2,\ 3, \ldots, \frac{m}{c}$$

weder a noch b als Factor enthalten. Nun haben wir oben gefunden, daſs die Reihe (I)

$$m\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

Zahlen enthält, die weder durch a, noch durch b theilbar sind; mithin enthält die Reihe (III)

$$\frac{m}{c}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

Zahlen derselben Beschaffenheit, d. h. es befinden sich in (I)

$$\frac{m}{c}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

Zahlen, die durch c, nicht aber auch durch a oder b theilbar sind. Werden auch diese Zahlen entfernt, so bleiben noch

$$m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)-\frac{m}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$$

$$=m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)$$

Zahlen, und diese enthalten weder a, noch b, noch c als Factor.

Durch Fortsetzung dieser Schlüsse ergiebt sich der Satz:

Wenn $m = a^\alpha b^\beta c^\gamma \ldots k^\varkappa$ ist, wo $a, b, c, \ldots k$ ungleiche Primzahlen bezeichnen, so ist

$$\varphi(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right).$$

Beispiel. Da $504 = 2^3 . 3^2 . 7$ ist, so ist

$$\varphi(504) = 504 . \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)$$

$$= \frac{504 . 1 . 2 . 6}{2 . 3 . 7} = 144,$$

d. h. es giebt 144 Zahlen, die prim zu 504 und nicht grösser als 504 sind.

§ 10. Eigenschaften der Function $\varphi(m)$. — **Lehrsatz I.** Sind $m_1, m_2, m_3, \ldots$ relative Primzahlen, d. h. Zahlen, von denen jede prim zu jeder anderen ist, so ist

$$\varphi(m_1 m_2 m_3 \ldots) = \varphi(m_1)\,\varphi(m_2)\,\varphi(m_3)\ldots$$

Beweis. Es seien

$a_1, b_1, c_1, \ldots$ die ungleichen Primzahlen von m_1,
$a_2, b_2, c_2, \ldots$ „ „ „ „ m_2,
$a_3, b_3, c_3, \ldots$ „ „ „ „ m_3,
. . . . ,

so ist nach § 9

$$\varphi(m_1) = m_1\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{b_1}\right)\cdots,$$

$$\varphi(m_2) = m_2\left(1-\frac{1}{a_2}\right)\left(1-\frac{1}{b_2}\right)\cdots,$$

. . . .

und ebenso

$$\varphi(m_1 m_2 m_3 \ldots)$$
$$= m_1 m_2 m_3 \ldots \left(1 - \frac{1}{a_1}\right)\left(1 - \frac{1}{b_1}\right) \cdots \left(1 - \frac{1}{a_2}\right) \cdots,$$

folglich

$$\varphi(m_1 m_2 m_3 \ldots) = \varphi(m_1)\,\varphi(m_2)\,\varphi(m_3) \ldots$$

Beispiele. $\varphi(\ 60) = \varphi(4)\,\varphi(3)\,\varphi(5) = 2 \,.\, 2 \,.\, 4 = \ 16,$
$\varphi(504) = \varphi(8)\,\varphi(9)\,\varphi(7) = 4 \,.\, 6 \,.\, 6 = 144.$

Lehrsatz II. Sind $d_1, d_2, \ldots, d_n$ sämmtliche Divisoren einer Zahl $m = a^\alpha b^\beta c^\gamma \ldots$, die Einheit und die Zahl selbst nicht ausgeschlossen, so ist

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_n) = m.$$

Beweis. Ein Divisor von m hat die Form

$$a^t\, b^u\, c^v \ldots,$$

wo t eine der Zahlen $0, 1, 2, \ldots, \alpha,$
„ u „ „ „ $0, 1, 2, \ldots, \beta,$
„ v „ „ „ $0, 1, 2, \ldots, \gamma,$
. . . .

bezeichnet, und da $a, b, c, \ldots$ ungleiche Primzahlen sind, so ist nach dem vorhergehenden Satze

$$\varphi(a^t\, b^u\, c^v \ldots) = \varphi(a^t)\,\varphi(b^u)\,\varphi(c^v) \ldots$$

Nun ist nach § 5 die Summe aller Divisoren von m gleich dem Produkt der Reihen

$$1 + a + a^2 + \cdots + a^\alpha,$$
$$1 + b + b^2 + \cdots + b^\beta,$$
. . . . ;

folglich die Summe der φ sämmtlicher Divisoren von m gleich dem Product der Reihen

$$\varphi(1) + \varphi(a) + \varphi(a^2) + \cdots + \varphi(a^\alpha),$$
$$\varphi(1) + \varphi(b) + \varphi(b^2) + \cdots + \varphi(b^\beta),$$
. . . .

Es ist aber

$$\varphi(1) = 1,$$
$$\varphi(a) = a\left(1 - \frac{1}{a}\right)$$
$$\varphi(a^2) = a^2\left(1 - \frac{1}{a}\right)$$
. . . .
$$\varphi(a^\alpha) = a^\alpha\left(1 - \frac{1}{a}\right),$$

also

$$\varphi(1) + \varphi(a) + \varphi(a^2) + \cdots + \varphi(a^\alpha)$$
$$= 1 + \left(1 - \frac{1}{a}\right)(a + a^2 + \cdots + a^\alpha) = a^\alpha.$$

Ebenso ergiebt sich

$$\varphi(1) + \varphi(b) + \varphi(b^2) + \cdots + \varphi(b^\beta) = b^\beta,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

mithin

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_n) = a^\alpha b^\beta \cdots = m.$$

Beispiel. Die Zahl 12 hat die 6 Divisoren 1, 2, 3, 4, 6, 12. Es ist

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2,$$
$$\varphi(6) = 2, \quad \varphi(12) = 4$$

und

$$1 + 1 + 2 + 2 + 2 + 4 = 12.$$

§ 11. Höchste Potenz einer Primzahl, welche in das Product aller Zahlen von 1 bis n aufgeht. (Legendre, théorie des nombres, Introduction, XVI). — Bezeichnet p eine Primzahl und r die gröfste ganze Zahl, welche in dem Bruche $\frac{n}{p}$ enthalten ist, so befinden sich in dem Produkte

$$P = 1 \,.\, 2 \,.\, 3 \ldots n$$

r durch p theilbare Factoren, nämlich p, $2p$, $3p$, ..., rp.

Ist ferner s die gröfste ganze Zahl, die der Bruch $\frac{n}{p^2}$ enthält, so giebt es in P s durch p^2 theilbare Factoren, nämlich p^2, $2p^2$, $3p^2$, ..., sp^2. Da wir nun aus jedem dieser Factoren p schon einmal genommen haben, so erhalten wir s neue Factoren p.

Bezeichnet weiter t die grösste in $\frac{m}{p^3}$ enthaltene ganze Zahl, so kommen noch t Factoren p hinzu.

So fahren wir fort, bis wir zu einem Bruche $\frac{m}{p^\varkappa}$ gelangen, der keine ganze Zahl mehr enthält. Die Summe der bei diesen successiven Divisionen gefundenen ganzen Quotienten ist der Exponent der höchsten Potenz von p, welche in das Produkt $1 \,.\, 2 \,.\, 3 \ldots n$ aufgeht.

Beispiel. Es ist

$$\frac{100}{2} = 50; \quad \frac{100}{4} = 25; \quad \frac{100}{8} = 12, \ldots; \quad \frac{100}{16} = 6, \ldots;$$

$$\frac{100}{32} = 3, \ldots; \quad \frac{100}{64} = 1, \ldots; \quad \frac{100}{128} = 0, \ldots,$$

und da

$$50 + 25 + 12 + 6 + 3 + 1 = 97$$

ist, so enthält das Produkt $1 . 2 . 3 \ldots 100$ den Factor 2^{97}.

Dieses Resultat setzt uns in den Stand, zu beweisen, dass der Ausdruck

$$\frac{1 . 2 . 3 \ldots a}{1 . 2 . 3 \ldots b . 1 . 2 . 3 \ldots c \ldots 1 . 2 \ldots d},$$

in welchem die ganzen Zahlen $a, b, c, \ldots, d$ der Bedingung

$$a = b + c + \cdots + d$$

genügen, eine ganze Zahl ist.

Wir haben nämlich nur darzuthun, dass eine beliebige Primzahl p in den Zähler dieses Ausdrucks mindestens ebenso oft aufgeht, als in den Nenner desselben. Zu diesem Zwecke bezeichnen wir mit Legendre die grösste in einem Bruche $\frac{x}{y}$ enthaltene ganze Zahl durch $E\left(\frac{x}{y}\right)$. Dann ist

$$E\left(\frac{b}{p}\right) + E\left(\frac{b}{p^2}\right) + \cdots + E\left(\frac{c}{p}\right) + E\left(\frac{c}{p^2}\right) + \cdots$$
$$+ \cdots + E\left(\frac{d}{p}\right) + E\left(\frac{d}{p^2}\right) + \cdots$$

der Exponent der höchsten Potenz von p, welche in den Nenner und

$$E\left(\frac{a}{p}\right) + E\left(\frac{a}{p^2}\right) + \cdots = E\left(\frac{b + c + \cdots + d}{p}\right)$$
$$+ E\left(\frac{b + c + \cdots + d}{p^2}\right) + \cdots$$

der Exponent der höchsten Potenz von p, welche in den Zähler aufgeht. Nun ist offenbar

$$E\left(\frac{b + c + \cdots + d}{p}\right) \geq E\left(\frac{b}{p}\right) + E\left(\frac{c}{p}\right) + \cdots + E\left(\frac{d}{p}\right)$$
$$E\left(\frac{b + c + \cdots + d}{p^2}\right) \geq E\left(\frac{b}{p^2}\right) + E\left(\frac{c}{p^2}\right) + \cdots + E\left(\frac{d}{p^2}\right)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

also geht jede Primzahl p, die in den Nenner aufgeht, mindestens ebenso oft in den Zähler auf, d. h. der Zähler ist durch den Nenner theilbar und der Ausdruck selbst eine ganze Zahl.

§ 12. Anzahl der Zahlen eines gegebenen Gebiets, welche durch gegebene Primzahlen nicht theilbar sind. — Wir stellen uns die Aufgabe zu ermitteln, wie viele Zahlen der Reihe

$$(1) \qquad 1, 2, 3, \ldots, n$$

durch gegebene Primzahlen $p, q, r, \ldots, s$ nicht theilbar sind.

Ist zunächst n ein Vielfaches von p, etwa $n = kp$, so enthält die Reihe (1) die k durch p theilbaren Zahlen

$$p, 2p, 3p, \ldots, kp;$$

mithin sind

$$n - k = n - \frac{n}{p} = n\left(1 - \frac{1}{p}\right)$$

Zahlen von (1) durch p nicht theilbar.

Wenn n kein Vielfaches von p ist und wir wieder die grösste in dem Bruche $\frac{n}{p}$ enthaltene ganze Zahl mit $E\left(\frac{n}{p}\right)$ bezeichnen, so ergiebt sich, dass die Reihe (1) $E\left(\frac{n}{p}\right)$ durch p theilbare, also

$$n - E\left(\frac{n}{p}\right)$$

Zahlen enthält, welche durch diese Primzahl nicht theilbar sind.

Um weiter zu bestimmen, wie viele von den Zahlen (1) weder durch p, noch durch q theilbar sind, scheiden wir zunächst die $E\left(\frac{n}{p}\right)$ durch p theilbaren, dann die $E\left(\frac{n}{q}\right)$ durch q theilbaren aus; dadurch würden wir

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right)$$

erhalten. Wir haben aber jede der $E\left(\frac{n}{pq}\right)$ durch das Produkt pq theilbaren Zahlen zweimal ausgeschieden. Es ergiebt sich somit, dass die Reihe (1)

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right) + E\left(\frac{n}{pq}\right)$$

Zahlen enthält, welche weder durch p, noch durch q theilbar sind. Wenn n durch pq theilbar ist, so geht dieser Ausdruck über in

$$n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Ist r eine dritte Primzahl, so ergiebt sich die Anzahl der weder durch p, noch durch q, noch durch r theilbaren Zahlen der Reihe (1) auf folgende Weise:

Wir lassen erst die durch p, dann die durch q, endlich die durch r theilbaren Zahlen weg und erhalten als Ausdruck für die Anzahl der zurückgebliebenen Zahlen

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right) - E\left(\frac{n}{r}\right).$$

Nun ist aber jede der beziehungsweise durch pq, qr, pr theilbaren Zahlen zweimal ausgeschieden; also muss zu obigem Ausdruck noch

$$E\left(\frac{n}{pq}\right) + E\left(\frac{n}{qr}\right) + E\left(\frac{n}{pr}\right)$$

addirt werden. Endlich ist jede der $E\left(\frac{n}{pqr}\right)$ Zahlen, die durch das Produkt pqr theilbar sind, dreimal fortgelassen (weil durch p, durch q und durch r theilbar), aber ebenso oft wieder hinzugefügt worden (weil durch pq, durch qr, durch pr theilbar). Da nun diese Zahlen aus (1) fortgelassen werden sollen, so ergiebt sich, dass die Reihe (1)

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right) - E\left(\frac{n}{r}\right) + E\left(\frac{n}{pq}\right) + E\left(\frac{n}{qr}\right) + E\left(\frac{n}{pr}\right) - E\left(\frac{n}{pqr}\right)$$

Zahlen enthält, welche weder durch p, noch durch q, noch durch r theilbar sind. Wenn n durch pqr theilbar ist, so geht dieser Ausdruck über in

$$n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right).$$

Durch Fortsetzung dieser Schlüsse erhalten wir den Satz:

Man erhält die Anzahl der Zahlen der Reihe

$1, 2, 3, \ldots, n$, welche durch keine der Primzahlen $p, q, r, \ldots, s$ theilbar sind, indem man das Produkt

$$n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right)$$

auflöst und jedes Glied unter Beibehaltung seines Vorzeichens durch die grösste in ihm enthaltene ganze Zahl ersetzt.

Wir wollen die Anzahl der Zahlen des Gebiets von 1 bis n, welche durch keine der i ersten Primzahlen

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \ldots, p_i$$

theilbar sind, durch $\varphi(n, i)$ bezeichnen. Es ist also z. B.

$$\varphi(7, 1) = 4, \quad \varphi(8, 1) = 4, \quad \varphi(10, 2) = 3,$$

u. s. w.

Es ist nun nicht schwer, eine Formel herzuleiten, welche die Berechnung von $\varphi(n, i)$ in allen Fällen ermöglicht.

Werden nämlich aus der Reihe (1) alle Zahlen weggelassen, welche durch eine der $i-1$ ersten Primzahlen theilbar sind, so bleiben noch $\varphi(n, i-1)$ Zahlen stehen.

Von diesen wollen wir noch diejenigen fortschaffen, welche durch die i^{te} Primzahl theilbar sind, so dass uns nach der Definition nur noch $\varphi(n, i)$ Zahlen übrig bleiben. Durch p_i theilbar sind von den Zahlen des betrachteten Gebiets

$$p_i, \; 2p_i, \; 3p_i, \; \ldots, \; E\left(\frac{n}{p_i}\right)p_i.$$

Ein Theil dieser Zahlen, nämlich die durch eine der $i-1$ ersten Primzahlen theilbaren, sind aber schon in Wegfall gekommen; es bleiben also nur noch die zu beseitigen, welche durch p_i, aber durch keine der vorhergehenden Primzahlen theilbar sind. Die Anzahl dieser Zahlen ist gleich der Anzahl der Zahlen der Reihe

$$1, 2, 3, \ldots, E\left(\frac{n}{p_i}\right),$$

welche durch keine der $i-1$ ersten Primzahlen theilbar sind, also gleich $\varphi\left[E\left(\frac{n}{p_i}\right), i-1\right]$, und somit ergiebt sich zur Berechnung von $\varphi(n, i)$ die Formel

$$(2) \qquad \varphi(n, i) = \varphi(n, i-1) - \varphi\left[E\left(\frac{n}{p_i}\right), i-1\right].$$

Aufgabe. Die Anzahl der Zahlen des Intervalls von 1 bis 1000 zu bestimmen, welche durch keine der vier ersten Primzahlen 2, 3, 5, 7 theilbar sind.

Es ist

$$\varphi(1000, 4) = \varphi(1000, 3) - \varphi(142, 3).$$

Nun ist

1) $\varphi(1000, 3) = \varphi(1000, 2) - \varphi(200, 2) = 333 - 67 = 266;$

denn

$$\varphi(1000, 2) = \varphi(1000, 1) - \varphi(333, 1) = 500 - 167 = 333$$

$$\varphi(200, 2) = \varphi(200, 1) - \varphi(66, 1) = 100 - 33 = 67.$$

2) $\varphi(142, 3) = \varphi(142, 2) - \varphi(28, 2) = 47 - 9 = 38;$

denn

$$\varphi(142, 2) = \varphi(142, 1) - \varphi(47, 1) = 71 - 24 = 47$$

$$\varphi(28, 2) = \varphi(28, 1) - \varphi(9, 1) = 14 - 5 = 9.$$

Es ergiebt sich also

$$\varphi(1000, 4) = 266 - 38 = 228,$$

d. h. das Gebiet 1, 2, ..., 1000 enthält 228 Zahlen, welche weder durch 2, noch durch 3, noch durch 5, noch durch 7 theilbar sind.

§ 13. Anzahl der Primzahlen in dem Intervall von 1 bis n. — Die Aufgabe, zu bestimmen, wie viele Primzahlen zwischen beliebig gegebenen Grenzen liegen, hat einige der bedeutendsten Mathematiker der neueren Zeit beschäftigt. Legendre (théorie des nombres, IV, 8), Gauss (Bd. II p. 444), Tchebichef (Liouville's Journal, Bd. 17), Riemann (Monatsberichte der Berliner Akademie, 1859) und Scheibner (Schlömilch's Journal, 1860) suchen die Anzahl der Primzahlen eines gegebenen Intervalls durch eine Formel auszudrücken. Dagegen hat Meissel (Mathematische Annalen, Bd. II u. III) die Aufgabe gelöst, die wirkliche Zählung der Primzahlen in einem gegebenen Gebiet zurückzuführen auf die Zählung derselben in einem kleineren Gebiet. Das Verfahren, welches Meissel einschlägt, wollen wir jetzt darlegen.

Es bezeichne $\psi(n)$ die Anzahl der Primzahlen in dem Intervall von 1 bis n, und es werde vorausgesetzt, man habe

die Anzahl der Primzahlen in den beiden Intervallen von 1 bis $\sqrt[3]{n}$ und von 1 bis $\sqrt{n}$ gefunden, also $\psi\sqrt[3]{n}$ und $\psi\sqrt{n}$ bestimmt. Da das zweite Intervall grösser als das erste ist, so wird es im Allgemeinen auch mehr Primzahlen als jenes enthalten. Wir setzen demgemäss

$$\psi\sqrt[3]{n} = m, \quad \psi\sqrt{n} = m + \mu,$$

wo $\mu > 0$ ist. Bezeichnet jetzt s eine Zahl, die der Bedingung $\mu > s > 0$ genügt, so liefert die Formel (2) des vorigen Paragraphen

$$(3)\quad \begin{cases} \varphi(n, m+s) \\ = \varphi(n, m+s-1) - \varphi\left(E\frac{n}{p_{m+s}}, m+s-1\right). \end{cases}$$

Nun ist p_m der Voraussetzung nach die grösste Primzahl des Intervalls von 1 bis $\sqrt[3]{n}$, also $\frac{\sqrt[3]{n}}{p_{m+1}} < 1$, und daraus ergiebt sich leicht

$$\frac{n}{p_{m+1}} < \sqrt[3]{n^2}, \quad \sqrt{\frac{n}{p_{m+1}}} < \sqrt[3]{n};$$

es ist also auch

$$\psi\sqrt{\frac{n}{p_{m+1}}} < \psi\sqrt[3]{n}, \quad \text{d. h.} \quad m > \psi\sqrt{\frac{n}{p_{m+1}}}.$$

Für den Werth $s = 1$ besteht demnach die Ungleichung

$$m + s - 1 > \psi\sqrt{\frac{n}{p_{m+s}}}.$$

Da nun, wenn s zunimmt, die linke Seite derselben offenbar grösser, die rechte Seite dagegen kleiner wird, so gilt diese Ungleichung für jedes $s \geq 1$.

Ferner enthält das Intervall von 1 bis $\sqrt{n}$ nach unserer Voraussetzung $m + \mu$ Primzahlen, von denen $p_{m+\mu}$ die grösste ist. Es ist also $p_{m+\mu} \leq \sqrt{n}$, folglich

$$\frac{1}{p_{m+\mu}} \geq \frac{1}{\sqrt{n}}, \quad \frac{n}{p_{m+\mu}} \geq \sqrt{n}$$

und somit

$$\psi\left(\frac{n}{p_{m+\mu}}\right) \geq \psi\sqrt{n}, \quad \text{d. h.} \quad \psi\left(\frac{n}{p_{m+\mu}}\right) \geq m + \mu > m + \mu - 1.$$

Für $s = \mu$ besteht demnach die Ungleichung

$$\psi\left(\frac{n}{p_{m+s}}\right) > m + s - 1\,,$$

und da bei abnehmendem s die linke Seite zunimmt, während die rechte kleiner wird, so gilt diese Ungleichung für jedes $s < \mu$.

Auf Grund unserer Voraussetzungen bestehen also für die Gültigkeit der Formel (3) die Grenzbedingungen

$$(4) \qquad \psi\left(\frac{n}{p_{m+s}}\right) > m + s - 1 > \psi\sqrt{\frac{n}{p_{m+s}}}\,,$$

wo $\mu \geq s > 0$ ist.

Ehe wir aus der Formel (3) weitere Schlüsse ziehen, wollen wir das zweite Glied ihrer rechten Seite etwas umformen.

Nach der Definition drückt $\varphi(n, a)$ die Anzahl der Zahlen des Gebiets von 1 bis n aus, welche durch keine der a ersten Primzahlen $p_1, p_2, \ldots, p_a$ theilbar sind. Es sind dies ausser der Einheit die Primzahlen $p_{a+1}, p_{a+2}, \ldots, p_{\psi(a)}$ und die Produktverbindungen der letzteren. Wird nun die Bedingung

$$(5) \qquad \psi(n) > a > \psi\sqrt{n}$$

gestellt, so ist $p_{a+1} > \sqrt{n}$, und folglich enthält das Intervall von p_{a+1} bis n keine Produktverbindung jener $\psi(n) - a$ Primzahlen; also ist unter der Bedingung (5)

$$(6) \qquad \varphi(n, a) = 1 + \psi(n) - a\,.$$

Diese Formel (6) darf auf den Fall

$$n = E\frac{n}{p_{m+s}}\,, \quad a = m + s - 1$$

angewandt werden, denn für diesen Fall fällt (4) mit der Bedingung (5) zusammen. Es ergiebt sich

$$\varphi\left(E\frac{n}{p_{m+s}}, m + s - 1\right) = 1 + \psi\left(\frac{n}{p_{m+s}}\right) - (m + s - 1)\,,$$

und dann geht (3) über in

$$\varphi(n, m + s) = \varphi(n, m + s - 1) - 2 + (m + s) - \psi\left(\frac{n}{p_{m+s}}\right).$$

Ertheilt man hierin s der Reihe nach die μ Werthe $\mu, \mu - 1, \mu - 2, \ldots, 2, 1$, so erhält man die μ Gleichungen

$$\varphi(n, m+\mu) = \varphi(n, m+\mu-1) - 2 + (m+\mu) - \psi\left(\frac{n}{p_{m+\mu}}\right),$$

$$\varphi(n, m+\mu-1) = \varphi(n, m+\mu-2) - 2 + (m+\mu) - 1 - \psi\left(\frac{n}{p_{m+\mu-1}}\right),$$

. . . .

$$\varphi(n, m+1) = \varphi(n, m) - 2 + (m+\mu) - (\mu-1) - \psi\left(\frac{n}{p_{m+1}}\right),$$

durch deren Addition sich

$$\varphi(n, m+\mu) = \varphi(n, m) - 2\mu + \mu(m+\mu) - \frac{\mu(\mu-1)}{2} - \left[\psi\left(\frac{n}{p_{m+1}}\right) + \psi\left(\frac{n}{p_{m+2}}\right) + \cdots + \psi\left(\frac{n}{p_{m+\mu}}\right)\right]$$

ergiebt. Nun ist $m + \mu = \psi\sqrt{n}$,

$$2\mu + \frac{\mu(\mu-1)}{2} = \frac{\mu(\mu+3)}{2};$$

also geht diese Formel, wenn

$$\psi\left(\frac{n}{p_{m+1}}\right) + \psi\left(\frac{n}{p_{m+2}}\right) + \cdots + \psi\left(\frac{n}{p_{m+\mu}}\right) = \sum_{s=1}^{s=\mu} \psi\left(\frac{n}{p_{m+s}}\right)$$

gesetzt wird, über in

$$(7) \quad \begin{cases} \varphi(n, \psi\sqrt{n}) = \varphi(n, m) + \mu\psi\sqrt{n} - \dfrac{\mu(\mu+3)}{2} \\ \qquad\qquad - \displaystyle\sum_{s=1}^{s=\mu} \psi\left(\frac{n}{p_{m+s}}\right). \end{cases}$$

Nach Formel (6) ist aber

$$\varphi(n, \psi\sqrt{n}) = 1 + \psi(n) - \psi\sqrt{n},$$

und durch Einsetzung dieses Werthes in (7) erhält man nach leichten Reductionen

$$(8) \quad \begin{cases} \psi(n) = \varphi(n, m) + m(\mu+1) + \dfrac{\mu(\mu-1)}{2} - 1 \\ \qquad\qquad - \displaystyle\sum_{s=1}^{s=\mu} \psi\left(\frac{n}{p_{m+s}}\right). \end{cases}$$

Diese Formel dient zur Berechnung der Anzahl der Primzahlen zwischen 1 und n.

Beispiel. Es sei $n = 1000$, so ist $\sqrt[3]{n} = 10$, $\sqrt{n} = 31$, $m = \psi(10) = 4$, $m + \mu = \psi\, 31 = 11$, $\mu = 7$; die Formel (8) liefert also

$$\psi(1000) = \varphi(1000, 4) + 4 \cdot 8 + \frac{7 \cdot 6}{2} - 1 - \sum_{s=1}^{s=7} \psi\left(\frac{1000}{p_{4+s}}\right).$$

Nun ist

$$p_5 = 11, \quad \psi\left(\frac{1000}{11}\right) = \psi(90) = 24,$$

$$p_6 = 13, \quad \psi\left(\frac{1000}{13}\right) = \psi(76) = 21,$$

$$p_7 = 17, \quad \psi\left(\frac{1000}{17}\right) = \psi(58) = 16,$$

$$p_8 = 19, \quad \psi\left(\frac{1000}{19}\right) = \psi(52) = 15,$$

$$p_9 = 23, \quad \psi\left(\frac{1000}{23}\right) = \psi(43) = 14,$$

$$p_{10} = 29, \quad \psi\left(\frac{1000}{29}\right) = \psi(34) = 11,$$

$$p_{11} = 31, \quad \psi\left(\frac{1000}{31}\right) = \psi(32) = 11,$$

also

$$\sum_{s=1}^{s=7} \psi\left(\frac{1000}{p_{4+s}}\right) = 112,$$

und da nach dem Früheren

$$\varphi(1000, 4) = 228$$

ist, so erhalten wir

$$\psi(1000) = 228 + 32 + 21 - 1 - 112 = 168;$$

zwischen 1 und 1000 giebt es also 168 Primzahlen.

Zweites Kapitel.

Congruente Zahlen.

§ 14. Definition. — Wenn die Differenz zweier Zahlen a, b durch eine dritte Zahl m theilbar, wenn also $\frac{a-b}{m}$ eine ganze Zahl ist, so nennt man a und b in Beziehung auf m congruent. Die Zahl m heisst dann der Modul, und man schreibt nach Gauss' Vorgange

$$a \equiv b \ (\text{mod. } m).$$

So ist z. B.

$$34 \equiv 16 \ (\text{mod. } 9), \ 17 \equiv -3 \ (\text{mod. } 10).$$

§ 15. Reste einer Zahl. — Erhält man bei der Division einer Zahl a durch m den Quotienten q und den Rest r, so ist

$$a = mq + r.$$

Dafür kann man aber auch

$$a = m(q+1) - (m-r)$$

schreiben, d. h. man kann den Quotienten um eine Einheit vergrössern und statt r den negativen Rest $-(m-r)$ nehmen. Wenn $r = \frac{m}{2}$ ist, so ist auch $m - r = \frac{m}{2}$, und wenn $r > \frac{m}{2}$ ist, so muss $m - r < \frac{m}{2}$ sein. Jede Zahl hat also in Beziehung auf einen Modul m einen positiven oder negativen Rest, welcher nicht grössser als $\frac{m}{2}$ ist. Diesen Rest nennt man den absolut kleinsten, im Gegensatz zu dem kleinsten positiven Rest, der eine der Zahlen 0, 1, 2, ..., $m - 1$ ist.

Beispiel. Dividirt man 24 durch 9, so erhält man als kleinsten positiven Rest 6, als absolut kleinsten Rest -3.

Es folgt nun aus der Annahme

$$a = mq + r,$$

dass $\frac{a-r}{m}$ eine ganze Zahl q ist, d. h. jede Zahl a ist ihrem Rest r in Beziehung auf den Divisor m als Modul congruent.

Von diesem Satze ausgehend, hat man den Begriff „Rest“ verallgemeinert und nennt jede von zwei für einen Modul congruenten Zahlen den Rest der andern für diesen Modul.

§ 16. Congruenzen. — Drückt man aus, dass zwei Grössen für einen Modul congruent sind, so erhält man eine Congruenz. Eine solche kann, wie eine Gleichung, eine oder mehrere Unbekannte enthalten und vom ersten, oder zweiten, u. s. w. Grade in Beziehung auf die Unbekannten sein. So ist

$$3x \equiv 7 \text{ (mod. 11)}$$

eine Congruenz ersten Grades mit einer Unbekannten,

$$5x + 2y \equiv 8 \text{ (mod. 13)}$$

eine Congruenz ersten Grades mit zwei Unbekannten,

$$x^2 + 3x \equiv 4 \text{ (mod. 7)}$$

eine Congruenz zweiten Grades mit einer Unbekannten, u. s. w.

§ 17. Sätze über die Verbindung von Congruenzen.

I. **Wenn zwei Zahlen a und b für einen Modul m einer dritten Zahl c congruent sind, so sind sie für denselben Modul einander congruent.**

Beweis. Da $a \equiv c$ (mod. m) und $b \equiv c$ (mod. m) sein soll, also $\frac{a-c}{m}$ und $\frac{b-c}{m}$ ganze Zahlen sind, so muss auch

$$\frac{a-c}{m} - \frac{b-c}{m} = \frac{a-b}{m}$$

eine ganze Zahl, d. h. $a \equiv b$ (mod. m) sein.

II. **Durch Addition mehrerer auf einen Modul bezüglichen Congruenzen erhält man eine für denselben Modul richtige Congruenz.**

Beweis. Ist

$$a_1 \equiv b_1,\ a_2 \equiv b_2,\ \ldots,\ a_n \equiv b_n \text{ (mod. } m),$$

also jede der Grössen

$$\frac{a_1 - b_1}{m}, \frac{a_2 - b_2}{m}, \ldots, \frac{a_n - b_n}{m}$$

eine ganze Zahl, so muss auch die Summe

$$\frac{a_1 - b_1}{m} + \frac{a_2 - b_2}{m} + \cdots + \frac{a_n - b_n}{m}$$
$$= \frac{(a_1 + a_2 + \cdots + a_n) - (b_1 + b_2 + \cdots + b_n)}{m}$$

eine ganze Zahl sein, d. h. es ist

$$a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod{m}.$$

Zusatz. Eine Congruenz bleibt richtig, wenn man jede Seite derselben mit einer Zahl n multiplicirt.

Beweis. Wird der vorhergehende Satz auf die n identischen Congruenzen

$$a \equiv b,\ a \equiv b, \ldots, a \equiv b \pmod{m}$$

angewandt, so ergiebt sich sofort

$$na \equiv nb \pmod{m}.$$

Oder: Wenn $a \equiv b \pmod{m}$, also $\frac{a - b}{m}$ eine ganze Zahl ist, so muss auch $\frac{an - bn}{m}$ eine ganze Zahl, d. h. $an \equiv bn \pmod{m}$ sein.

Beispiele. Aus den Congruenzen

$$17 \equiv 5,\ 19 \equiv -5,\ 34 \equiv 10 \pmod{12}$$

folgt durch Addition

$$70 \equiv 10 \pmod{12}.$$

Aus $5 \equiv -2 \pmod{7}$ folgt durch Multiplication mit 3

$$15 \equiv -6 \pmod{7}.$$

III. Die Differenz zweier auf einen Modul bezüglichen Congruenzen ist eine für denselben Modul richtige Congruenz.

Beweis. Wenn $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{m}$, also $\frac{a_1 - b_1}{m}$, $\frac{a_2 - b_2}{m}$ ganze Zahlen sind, so ist auch

$$\frac{a_1 - b_1}{m} - \frac{a_2 - b_2}{m} = \frac{(a_1 - a_2) - (b_1 - b_2)}{m}$$

eine ganze Zahl, d. h.

$$a_1 - a_2 \equiv b_1 - b_2 \pmod{m}.$$

Beispiel. Aus

$$17 \equiv 5,\ 19 \equiv -5 \pmod{12}$$

folgt

$$-2 \equiv 10 \pmod{12}.$$

IV. Das Produkt mehrerer auf einen Modul bezüglichen Congruenzen ist eine für denselben Modul richtige Congruenz.

Beweis. Ist $a_1 \equiv b_1 \pmod{m}$, also $\frac{a_1 - b_1}{m} = g_1$, wo g_1 eine ganze Zahl bezeichnet, so ergiebt sich

$$(1) \qquad a_1 = b_1 + mg_1 .$$

Ebenso kann man statt der übrigen gegebenen Congruenzen

$$a_2 \equiv b_2,\ a_3 \equiv b_3,\ \ldots,\ a_n \equiv b_n \pmod{m}$$

die Gleichungen

$$(2) \qquad a_2 = b_2 + mg_2,\ \ldots,\ a_n = b_n + mg_n$$

setzen, wo auch $g_2, \ldots, g_n$ ganze Zahlen bedeuten. Durch Multiplication der Gleichungen (1) und (2) erhält man

$$a_1 a_2 a_3 \cdots a_n = b_1 b_2 b_3 \cdots b_n + mG,$$

wo G eine ganze Zahl bezeichnet, auf deren Grösse es uns hier nicht ankommt. Es ist mithin

$$\frac{a_1 a_2 a_3 \cdots a_n - b_1 b_2 \cdots b_n}{m} = G,$$

d. h.

$$a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n \pmod{m}.$$

Zusatz. Eine Congruenz bleibt richtig, wenn man beide Seiten auf dieselbe Potenz erhebt.

Beweis. Wird in der letzten Congruenz

$$a_1 = a_2 = a_3 = \cdots = a_n = a$$

$$b_1 = b_2 = b_3 = \cdots = b_n = b$$

vorausgesetzt, so geht dieselbe über in

$$a^n \equiv b^n \pmod{m}.$$

Beispiele. Aus $12 \equiv 5,\ 3 \equiv -4,\ 2 \equiv -5 \pmod{7}$ folgt durch Multiplication

$$72 \equiv 100 \pmod{7}.$$

Aus $2 \equiv -5 \pmod{7}$ folgt durch Erhebung auf die 2[te] Potenz

$$4 \equiv 25 \pmod{7}.$$

V. **Wenn beide Glieder a, b einer Congruenz**

$$a \equiv b \pmod{m}$$

einen grössten gemeinschaftlichen Divisor d haben, der prim zum Modul m ist, so erhält man eine für denselben Modul m richtige Congruenz, wenn man beiderseits durch d dividirt.

Haben aber d und der Modul m den grössten gemeinschaftlichen Divisor δ, so gilt die durch jene Division erhaltene neue Congruenz nur noch für den Modul $\frac{m}{\delta}$.

Beweis. Es sei $a = \alpha d$, $b = \beta d$, wo α und β prim zu einander sind. Nun soll

$$\frac{\alpha d - \beta d}{m} = \frac{d(\alpha - \beta)}{m}$$

eine ganze Zahl sein. Wenn also d prim zu m ist, so muss (§ 7) m in $\alpha - \beta$ aufgehen, also

$$\alpha \equiv \beta \pmod{m}$$

sein. Wenn aber d und m den grössten gemeinschaftlichen Divisor δ haben, so lässt sich der Bruch $\frac{d(\alpha - \beta)}{m}$ durch δ heben und geht, wenn $d = d_1 \delta$, $m = m_1 \delta$ gesetzt wird, über in $\frac{d_1(\alpha - \beta)}{m_1}$. Damit dieser Ausdruck eine ganze Zahl sei, muss, da m_1 prim zu d_1 ist, $\frac{\alpha - \beta}{m_1}$ eine ganze Zahl, d. h.

$$\alpha \equiv \beta \pmod{m_1}$$

sein.

Beispiele. Aus $26 \equiv 12 \pmod{7}$ folgt, da 2 prim zu 7 ist,

$$13 \equiv 6 \pmod{7}.$$

Aber aus $28 \equiv 16 \pmod{6}$ folgt

$$7 \equiv 4 \text{ (mod. 3, **nicht** mod. 6)}.$$

§ 18. Anwendungen dieser Sätze. — Die vorhergehenden Sätze finden im bürgerlichen Rechnen vielfache Anwendung. Zunächst ergeben sich aus ihnen die verschiedenen Regeln, nach denen man entscheidet, ob eine Zahl durch eine andere theilbar sei oder nicht. Es sei nämlich P eine Zahl, welche a Einer, b Zehner, c Hunderte, u. s. w. enthält, also

$$P = a + 10b + 100c + \cdots$$

Ist dann für einen Modul m

$$10 \equiv r_1,\ 100 \equiv r_2,\ \ldots,$$

so ist

$$P \equiv a + r_1 b + r_2 c + \cdots \pmod{m},$$

und wenn letztere Zahl durch m theilbar ist, so ist auch P durch m theilbar.

Beispiele. I. Sowohl für den Modul 2, als auch für den Modul 5 ist

$$10 \equiv 0,\ 100 \equiv 0,\ \ldots,$$

mithin

$$P \equiv a\ (\text{mod}.\ 2 \text{ und mod}.\ 5),$$

und dies drückt aus, dass eine Zahl durch 2 oder 5 theilbar ist, wenn die Anzahl ihrer Einer durch 2 oder 5 theilbar ist.

II. Sowohl für den Modul 3, als auch für den Modul 9 ist

$$10 \equiv 1,\ 100 \equiv 1,\ \ldots,$$

mithin

$$P \equiv a + b + c + \cdots\ (\text{mod}.\ 3 \text{ und mod}.\ 9),$$

und diese Formel lehrt, dass jede Zahl bei der Division durch 3 und durch 9 denselben Rest wie ihre Quersumme lässt.

III. Für den Modul 11 ist

$$10 \equiv -1,\ 100 \equiv +1,\ 1000 \equiv -1,\ \text{u. s. w.},$$

folglich ist

$$P \equiv a - b + c - d + \cdots \pmod{11},$$

welche Formel die bekannte Theilbarkeitsregel für den Divisor 11 liefert.

IV. Für den Modul 7 ist

$$10^0 \equiv 1,\ 10^1 \equiv 3,\ 10^2 \equiv 2,\ 10^3 \equiv -1,\ 10^4 \equiv -3,$$
$$10^5 \equiv -2,\ 10^6 \equiv 1,\ 10^7 \equiv 3,\ \ldots,$$

also

$$P \equiv (a + 3b + 2c) - (d + 3e + 2f) + \cdots \pmod{7}.$$

Nach dieser Formel ist z. B.

$$37589 \equiv (9 + 24 + 10) - (7 + 9) \equiv 27 \equiv 6\ (\text{mod}.\ 7),$$
$$275\,768\,929 \equiv (9 + 6 + 18) - (8 + 18 + 14) + (5 + 21 + 4)$$
$$\equiv 33 - 40 + 30 \equiv 23 \equiv 2 \pmod{7}.$$

V. Es sei jetzt und in den folgenden Beispielen

$$P = a + 10b,$$

wo a die Anzahl der Einer und b die Zahl bezeichnet, die aus P bei Fortlassung der Einer entsteht. Da nun

$$1 \equiv 8,\ 10 \equiv -4 \ (\text{mod. } 7)$$

ist, so ist

$$P \equiv 8a - 4b \equiv -4(b - 2a) \ (\text{mod. } 7),$$

und da -4 prim zu 7 ist, so wird P durch 7 theilbar sein, wenn $b - 2a$ durch 7 theilbar ist.

Danach ist 2422 durch 7 theilbar, wenn 7 in $242 - 4 = 238$ aufgeht,
„ 238 „ „ , „ „ $23 - 16 = 7$ „ ,
und da 7 durch 7 theilbar ist, so ist auch 2422 durch 7 theilbar.

VI. Für den Modul 13 ist

$$1 \equiv -12,\ 10 \equiv -3,$$

also

$$P \equiv -12a - 3b \equiv -3(b + 4a) \ (\text{mod. } 13),$$

und P wird durch 13 theilbar sein, wenn 13 in $b + 4a$ aufgeht.

Untersucht man mit Rücksicht hierauf die Zahl 701064, so erhält man der Reihe nach die neuen Zahlen

$$70122,\ 7020,\ 702,\ 78,$$

und da 13 in 78 aufgeht, so ist auch jede der vorhergehenden Zahlen durch 13 theilbar.

VII. Für den Modul 19 ist

$$1 \equiv -18,\ 10 \equiv -9,$$

also

$$P \equiv -18a - 9b \equiv -9(b + 2a) \ (\text{mod. } 19).$$

Bei Anwendung der sich hieraus ergebenden Regel erhält man aus 16536194 der Reihe nach die neuen Zahlen

$$1653627,\ 165376,\ 16549,\ 1672,\ 171,\ 19,$$

und da die letzte durch 19 theilbar ist, so sind es auch alle vorhergehenden.

VIII. Wird weiter $P = a + 100b$ gesetzt, wo a die aus den Einern und Zehnern gebildete (zweistellige) Zahl, b die Zahl ist, in welche P sich verwandelt, wenn a fortgelassen wird, so folgt aus den beiden Congruenzen

$$100 \equiv 2 \ (\text{mod. } 7) \quad \text{und} \quad 100 \equiv -2 \ (\text{mod. } 17),$$

dass

$$P \equiv a + 2b \ (\text{mod. } 7) \quad \text{und} \quad P \equiv a - 2b \ (\text{mod. } 17)$$

ist. Die erste dieser Formeln liefert eine neue Theilbarkeitsregel für 7, die zweite eine solche für 17; bei Anwendung der letzteren ist, wenn $2b > a$ ist, die rechte Seite durch $-(2b - a)$ zu ersetzen.

Beispiele. Um zu sehen, ob 5943 durch 7 theilbar sei, hat man die Zahlen $43 + 118 = 161$, $61 + 2 = 63$ zu bilden. Da 63 durch 7 theilbar ist, so ist es auch die vorgelegte Zahl.

Dass 8041 durch 17 theilbar ist, erkennt man durch Bildung der Zahlen $160 - 41 = 119$, $19 - 2 = 17$.

In ähnlicher Weise könnte man für andere Divisoren Regeln herleiten; doch ist es meist zweckmässiger, die Division selbst zu versuchen, als solche Regeln anzuwenden.

Die oben hergeleiteten Sätze lassen noch eine andere Anwendung zu. Hat man nämlich eine Reihe von Zahlen durch Addition, Subtraction oder Multiplication vereinigt, so kann man, um das Resultat zu prüfen, jede Zahl durch ihren kleinsten Rest für irgend einen Modul (am zweckmässigsten 9 oder 11) ersetzen. Vereinigt man dann diese Reste in der vorgeschriebenen Weise, so muss das so erhaltene Resultat, wenn kein Fehler begangen ist, denselben Rest wie das durch Vereinigung der Zahlen selbst erhaltene liefern.

Um z. B. zu sehen, ob wirklich

$$(27 + 46)\,39 - 112 = 2735$$

sei, ersetze man links jede Zahl durch ihren Rest für den Modul 9; man erhält $(0 + 1)\,3 - 4 = -1 \equiv 8 \pmod{9}$, welchen Rest auch $2735 \equiv 2 + 7 + 3 + 5 = 17$ liefert. Ersetzt man jede Zahl links durch ihren Rest für den Modul 11, so erhält man

$$(5 + 2)\,6 - 2 = 40 \equiv 7 \pmod{11},$$

und denselben Rest hat auch

$$2735 \equiv (5 + 7) - (3 + 2) = 7 \pmod{11}.$$

§ 19. Wurzeln von Congruenzen. — Bezeichnen A, B, $C, \ldots, N$, P gegebene ganze Zahlen und n eine positive ganze Zahl, so ist

$$Ax^n + Bx^{n-1} + \ldots + Nx + P \equiv 0 \pmod{m}$$

eine Congruenz n^{ten} Grades mit einer Unbekannten x. Wenn

jeder der Coefficienten $A, B, \ldots, N, P$ durch den Modul m theilbar ist, so wird die Congruenz durch jeden Werth von x befriedigt; in diesem Falle nennt man sie eine identische Congruenz. Die Congruenz ist unmöglich, d. h. es kann keinen Werth von x geben, der ihr genügt, wenn alle Coefficienten, mit Ausnahme von P, durch m theilbar sind.

Wenn weder das eine, noch das andere der Fall und x_1 eine Zahl ist, nach deren Einsetzung an die Stelle von x die linke Seite der Congruenz durch m theilbar ist, so nennt man x_1 eine Wurzel der Congruenz. So ist 2 eine Wurzel der Congruenz $3x + 7 \equiv 0$ (mod. 13), da $3 \cdot 2 + 7 = 13$ durch 13 theilbar ist.

Hat eine auf den Modul m bezügliche Congruenz eine Wurzel x_1, so wird sie, wie die in § 17 bewiesenen Sätze erkennen lassen, auch durch jede der unendlich vielen Zahlen befriedigt, welche $\equiv x_1$ (mod. m) sind. So wird die linke Seite der vorigen Congruenz, welche eine Wurzel 2 hat, durch 13 theilbar, wenn man x durch irgend eine der Zahlen 2, 15, 28, ..., oder -11, -24, ..., allgemein $2 + 13k$ ersetzt, wo k jede ganze positive oder negative Zahl sein kann. Alle diese Zahlen sieht man aber nur als eine einzige Wurzel an, und die verschiedenen Wurzeln einer Congruenz bestimmen, heisst die incongruenten Zahlen ermitteln, welche derselben genügen.

Enthält eine Congruenz mehrere Unbekannte $x, y, \ldots$, oder liegen mehrere Congruenzen mit mehreren Unbekannten vor, so bilden die zusammengehörigen Werthe $x_1, y_1, \ldots$, welche im ersteren Falle der Congruenz, im zweiten Falle allen Congruenzen genügen, eine Auflösung derselben.

Beispiele. Eine Auflösung der Congruenz

$$3x + 5y + 6 \equiv 0 \pmod{17}$$

ist

$$x \equiv 2,\ y \equiv 1 \pmod{17}.$$

Eine Auflösung der Congruenzen

$$\left.\begin{aligned} 13x - 7y - 10 &\equiv 0 \\ 6x + 9y + 11 &\equiv 0 \end{aligned}\right\} \pmod{16}$$

ist

$$x \equiv 3,\ y \equiv 11 \pmod{16}.$$

§ **20.** Umformung einer Congruenz. — Man kann eine Congruenz

$$Ax^n + Bx^{n-1} + \ldots + Nx + P \equiv 0 \ (\text{mod. } m)$$

dadurch auf eine andere Form bringen, dafs man jeden ihrer Coefficienten A, B, ..., N, P durch seinen kleinsten Rest für den Modul m ersetzt. Die Zulässigkeit dieser Umformung ergiebt sich aus § 17. So ist die Congruenz

$$17x^4 + 12x^3 + 25x^2 + 20x + 49 \equiv 0 \ (\text{mod. } 12)$$

gleichbedeutend mit

$$5x^4 + x^2 - 4x + 1 \equiv 0 \ (\text{mod. } 12).$$

Drittes Kapitel.

Congruenzen ersten Grades.

§ 21. Bedingung für die Möglichkeit einer Congruenz ersten Grades mit einer Unbekannten. — Jede Congruenz ersten Grades mit einer Unbekannten lässt sich auf die Form

$$ax \equiv b \pmod{m}$$

bringen, wo x die Unbekannte, a und b gegebene ganze Zahlen bezeichnen, von denen jede (§ 20) kleiner als der Modul m vorausgesetzt werden kann.

Lehrsatz I. Wenn a prim zu m ist, so hat die Congruenz $ax \equiv b \pmod{m}$ stets eine, aber auch nur eine Wurzel.

Beweis. Wir betrachten die Reihe der Produkte

$$a,\ 2a,\ 3a,\ \ldots,\ (m-1)\,a.$$

Wäre eins derselben, etwa ka durch m theilbar, so müsste, da a prim zu m ist, k durch m theilbar sein (§ 7, Lehrsatz I), was offenbar unmöglich ist. Ferner sind jene Produkte für den Modul m sämmtlich incongruent; denn hätte man $ka \equiv k'a \pmod{m}$, so wäre (§ 17, V) auch

$$k \equiv k' \pmod{m},$$

während zwei verschiedene Zahlen der Reihe $1, 2, 3, \ldots, (m-1)$, durch m dividirt, nicht denselben Rest geben können. Da somit die $m-1$ Produkte für den Modul m sämmtlich verschiedene Reste geben, und da der Rest Null ausgeschlossen ist, so müssen ihre Reste in irgend einer Reihenfolge mit den Zahlen $1, 2, 3, \ldots, (m-1)$ übereinstimmen, dergestalt dass jedes Produkt einer, aber auch nur einer dieser Zahlen congruent ist. Unter den letzteren befindet sich auch b. Es

giebt also eine einzige Zahl x, welche, mit a multiplicirt, für den Modul m den Rest b liefert, d. h. der gegebenen Congruenz genügt.

Anmerkung. Wenn der Modul eine Primzahl ist, so ist die Bedingung des vorhergehenden Satzes stets erfüllt.

Lehrsatz II. Die Congruenz $ax \equiv b \pmod{m}$ ist unmöglich, wenn der grösste gemeinschaftliche Divisor d von a und m nicht auch in b aufgeht.

Beweis. Die gegebene Congruenz ist der Gleichung

$$ax = b + my$$

äquivalent, wo y eine beliebige ganze Zahl bezeichnet. Hieraus erhält man $ax - my = b$, oder durch Division mit d

$$\frac{a}{d}x - \frac{m}{d}y = \frac{b}{d}.$$

Die linke Seite dieser Gleichung ist der Voraussetzung nach eine ganze Zahl. Die Gleichung und daher auch die Congruenz ist somit unmöglich, wenn $\frac{b}{d}$ ein Bruch ist, d. h. wenn d nicht auch in b aufgeht.

Lehrsatz III. Wenn der grösste gemeinschaftliche Divisor d von a und m auch in b aufgeht, so hat die Congruenz $ax \equiv b \pmod{m}$ d incongruente Wurzeln.

Beweis. Nach § 17, V geht die vorgelegte Congruenz über in

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\text{mod.}\ \frac{m}{d}\right).$$

Da nun $\frac{a}{d}$ prim zu $\frac{m}{d}$ ist, so hat diese letztere Congruenz eine einzige Wurzel (nach Lehrsatz I), die wir x_1 nennen wollen. Die gegebene Congruenz hat dann die d verschiedenen (d. i. nach dem Modul m incongruenten) Wurzeln

$$x_1,\ x_1 + \frac{m}{d},\ x_1 + \frac{2m}{d},\ \ldots,\ x_1 + \frac{(d-1)m}{d}.$$

Beispiele. Die Congruenz $5x \equiv 7 \pmod{12}$ hat nur die Wurzel $x \equiv -1 \pmod{12}$.

Die Congruenz $6x \equiv 7 \pmod{12}$ ist unmöglich.

Die Congruenz $9x \equiv 6 \pmod{15}$ ist möglich, weil der grösste gemeinschaftliche Divisor von 9 und 15, d. i. 3, auch

in 6 aufgeht. Durch Division mit 3 erhält man die Congruenz

$$3x \equiv 2 \pmod{5},$$

welche nur die eine Wurzel

$$x \equiv -1 \pmod{5}$$

hat; die vorgelegte Congruenz hat also die drei verschiedenen Wurzeln

$$x_1 \equiv -1, \quad x_2 \equiv -1 + 5 = 4,$$
$$x_3 \equiv -1 + 10 = 9 \pmod{15}.$$

§ 22. Auflösung der Congruenz ersten Grades mit einer Unbekannten. — Nachdem wir untersucht haben, unter welcher Bedingung die Congruenz $ax \equiv b \pmod{m}$ möglich ist, und wie viele Wurzeln sie in jedem Falle hat, wollen wir diese Wurzeln bestimmen lernen. Wir können dabei von vorn herein a als prim zu m annehmen; denn ein etwa vorhandener gemeinschaftlicher Divisor würde sich (§ 21, Lehrsatz III) durch Division entfernen lassen.

Die vorgelegte Congruenz ist gleichbedeutend mit der Gleichung

$$ax = b + my,$$

wenn darin y eine ganze Zahl bedeutet. Diese Gleichung ist unbestimmt, da sie zwei Unbekannte x, y enthält. Sie lässt im Allgemeinen unendlich viele Lösungen zu; denn man kann der einen Unbekannten jeden beliebigen Werth beilegen und sodann mittels der Gleichung den Werth der andern Unbekannten berechnen. Wenn man sich aber auf ganze und (wie es meist geschieht) positive Werthe der Unbekannten beschränkt, so wird die Anzahl der Lösungen verringert. Oft sind in den Aufgaben, die zu unbestimmten Gleichungen führen, und die man nach dem Mathematiker Diophant, welcher sich zuerst mit solchen Aufgaben beschäftigt hat, diophantische Aufgaben nennt, noch Bedingungen angegeben, die sich zwar nicht in Gleichungen umsetzen lassen, aber doch die Zahl der Lösungen noch weiter verringern.

Wir wollen jetzt die ganzen Zahlen bestimmen, welche, für x eingesetzt, der Gleichung genügen. Durch Division mit a erhält man

$$x = c + dy + \frac{e + fy}{a},$$

wo c und d die Quotienten, e und f die Reste der Division von beziehungsweise b und m durch a bezeichnen. Da nun x, c, d, y ganze Zahlen sind, so muss auch $\frac{e + fy}{a}$ eine ganze Zahl sein. Wir setzen also, diese Zahl mit z bezeichnend,

$$\frac{e + fy}{a} = z$$

und erhalten daraus

$$y = \frac{-e + az}{f},$$

oder, wenn wir die Division mit f in $-e$ und a ausführen und die Quotienten mit g und h, die Reste mit i und k bezeichnen,

$$y = g + hz + \frac{i + kz}{f}.$$

Mit dem Bruche $\frac{i + kz}{f}$, der wieder eine ganze Zahl sein muss, da y, g, h, z ganze Zahlen sind, verfahren wir ebenso, wie wir mit $\frac{e + fy}{a}$ verfuhren, und da die Brüche, zu denen die Fortsetzung dieses Verfahrens führt, immer kleinere Zahlen zu Nennern haben ($a > f >$ u. s. w.), so müssen wir endlich zu einem Bruch mit dem Nenner 1 gelangen. Die zuletzt erhaltene Gleichung bestimmt dann die vorletzte der Unbekannten $x, y, z, \ldots$ mittels der letzten, die unbestimmt bleibt, und durch eine Reihe von Substitutionen lassen sich rückwärts alle vorhergehenden Unbekannten, also zuletzt auch x, durch dieselbe Unbestimmte ausdrücken.

Die Rechnung wird zuweilen erheblich abgekürzt, wenn man die absolut kleinsten Reste nimmt.

Beispiel. Die Congruenz $15x \equiv 11 \pmod{23}$ ist der Gleichung

$$15x = 11 + 23y$$

äquivalent. Diese liefert der Reihe nach

$$x = 1 + 2y - \frac{4 + 7y}{15},$$

$$\frac{4 + 7y}{15} = z, \quad y = \frac{-4 + 15z}{7} = 2z + \frac{z - 4}{7}, \quad \frac{z - 4}{7} = u,$$

$$z = 4 + 7u,$$

und hieraus folgt

$$y = 8 + 15u,$$
$$x = 13 + 23u.$$

Die Congruenz hat also die Wurzel

$$x \equiv 13 \pmod{23}.$$

Anmerkung I. — Das oben dargelegte Verfahren rührt von Euler her (Algebra II, Kap. I). Von den anderen Methoden, eine Gleichung ersten Grades mit 2 Unbekannten zu lösen, sei noch die von Lagrange erwähnt, welche auf den Eigenschaften der Näherungswerthe von Kettenbrüchen beruht, und die wir in § 38 kennen lernen werden.

Anmerkung II. — Wenn der Modul m der Congruenz

$$ax \equiv b \pmod{m}$$

nicht sehr gross ist, so verfährt man zweckmässig auf folgende Weise: Man schreibt die Reihe der Zahlen hin, welche für den Modul m den Rest b geben, und wählt die kleinste dieser Zahlen, die durch a theilbar ist. Ist c diese Zahl, so hat die Congruenz die Wurzel $\frac{c}{a}$.

Es soll z. B. die Congruenz $5x \equiv 8 \pmod{11}$ gelöst werden. Die Zahlen, die durch 11 dividirt, den Rest 8 haben, sind 8, 19, 30, ...; die gesuchte Wurzel ist also $\frac{30}{5} = 6$.

Anmerkung III. Durch geeignete Anwendung der in § 17 bewiesenen Sätze kann man eine vorgelegte Congruenz so transformiren, dass der Coefficient schliesslich gleich 1 wird. Da dieses Verfahren in vielen Fällen leicht und schnell zum Ziele führt, so wollen wir einige Beispiele nach demselben behandeln.

1. Beispiel. $35x \equiv 78 \pmod{97}$.

Da $35 \equiv -62 \pmod{97}$ ist, so erhalten wir

$$-62x \equiv 78 \pmod{97}$$

und weiter durch Division mit 2

$$-31x \equiv 39 \pmod{97}.$$

Wird diese Congruenz zur vorgelegten addirt, so folgt

$$4x \equiv 117 \equiv 20 \pmod{97},$$

und hieraus ergiebt sich durch Division mit 4

$$x \equiv 5 \pmod{97}.$$

2. Beispiel. $39x \equiv 7 \pmod{28}$.

$$11x \equiv 7 \pmod{28},$$

$$55x \equiv 35 \pmod{28},$$

$$-x \equiv 7 \pmod{28},$$

$$x \equiv -7 \equiv 21 \pmod{28}.$$

3. Beispiel. $35x \equiv 12 \pmod{88}$.

Da x durch 4 theilbar sein muss, so setzen wir

$$x = 4y$$

und erhalten

$$35y \equiv 3 \pmod{22},$$
$$-9y \equiv 3 \pmod{22},$$
$$3y \equiv -1 \equiv 21 \pmod{22},$$
$$y \equiv 7 \pmod{22},$$
$$x \equiv 28 \pmod{88}.$$

§ 23. Abkürzung der Rechnung bei zusammengesetzten Moduln. — Wenn der Modul eine zusammengesetzte Zahl $m \, . \, n$ ist, wo m eine Primzahl, n eine beliebige Zahl bezeichnen möge, so lässt sich die Auflösung der Congruenz

$$(1) \qquad ax \equiv b \pmod{mn}$$

vereinfachen. Da $ax - b$ durch mn theilbar sein soll, so muss zunächst auch m in $ax - b$ aufgehen, d. h.

$$(2) \qquad ax \equiv b \pmod{m}$$

sein. Ist x_1 eine Wurzel dieser Congruenz (2), so ist

$$x = x_1 + my,$$

wo y eine Unbestimmte bezeichnet, die allgemeine Form der Wurzeln von (1). Es genügt aber nicht jede in diesem Ausdruck enthaltene Zahl der Congruenz (1), sondern nur die Zahlen, welche gewissen Werthen von y entsprechen. Um diese Werthe von y zu bestimmen, ersetzen wir in (1) x durch $x_1 + my$ und erhalten

$$amy \equiv b - ax_1 \pmod{m \, . \, n}$$

oder, da $b - ax_1$ durch m theilbar ist, durch Division mit m

$$(3) \qquad ay \equiv c \pmod{n},$$

wo $c = \frac{b - ax_1}{m}$ gesetzt ist.

Die Congruenz (3) liefert den Werth (resp. die Werthe) von y, durch dessen Einsetzung in $x = x_1 + my$ sich der Werth von x ergiebt.

Wenn auch der Modul n der Congruenz (3) eine zusammengesetzte Zahl ist, so kann man mit (3) ebenso verfahren,

wie wir mit (1) verfuhren. Auf diese Weise lässt sich die Auflösung einer Congruenz ersten Grades auf die von Congruenzen zurückführen, von denen jede eine Primzahl zum Modul hat.

Beispiel. Um die Congruenz

$$(1) \qquad 19x \equiv 3 \pmod{44}$$

zu lösen, behandeln wir zunächst

$$(2) \qquad 19x \equiv 3 \pmod{2}$$

und erhalten $x \equiv 1 \pmod{2}$, d. h. $x = 1 + 2y$.

Wird dieser Werth von x in (1) eingesetzt, so folgt

$$19 + 38y \equiv 3 \pmod{44}$$

oder

$$(3) \qquad 19y \equiv -8 \pmod{22}.$$

Auch diese Congruenz lösen wir zunächst für den Modul 2, behandeln also

$$(4) \qquad 19y \equiv -8 \pmod{2}$$

und erhalten $y \equiv 0 \pmod{2}$, d. h. $y = 2z$. Für diesen Werth von y geht (3) über in $38z \equiv -8 \pmod{22}$ oder

$$19z \equiv -4 \pmod{11} \quad \text{oder} \quad 8z \equiv -4 \pmod{11}$$

oder endlich

$$(5) \qquad 2z \equiv -1 \pmod{11}.$$

Diese Congruenz ist gleichbedeutend mit

$$2z \equiv 10 \pmod{11},$$

welche $z \equiv 5 \pmod{11}$ liefert.

Es ist also

$$z = 5 + 11k, \qquad y = 2z = 10 + 22k$$

und

$$x = 1 + 2y = 21 + 44k,$$

d. h. die Congruenz (1) hat die Wurzel

$$x \equiv 21 \pmod{44}.$$

§ 24. Aufgaben. — 1. Jemand kauft Pferde und Ochsen, zusammen für 10820 Mk. Er bezahlt für ein Pferd 760 Mk., für einen Ochsen 340 Mk. Wie viel Pferde und wie viel Ochsen hat er gekauft?

Bezeichnet x die Anzahl der Pferde, y die der Ochsen, so ist

$$760x + 340y = 10\,820 \quad \text{oder} \quad 38x + 17y = 541\,.$$

Statt dieser Gleichung setzen wir die Congruenz

$$38x \equiv 541 \text{ (mod. 17)},$$

welche $4x \equiv 14$ (mod. 17), also

$$2x \equiv 7 \text{ (mod. 17)}$$

ergiebt und die Wurzel $x \equiv 12$ (mod. 17) hat, so dass wir

$$x = 12 + 17k$$

zu setzen haben, wo k eine ganze Zahl bezeichnet. Wird dieser Werth von x in die Gleichung

$$38x + 17y = 541$$

eingesetzt, so erhält man

$$456 + 38 \,.\, 17k + 17y = 541\,,$$

also $y = 5 - 38k$, und damit sowohl x wie auch y positiv sei, muss $k = 0$ angenommen werden. Die Aufgabe lässt also nur die eine Lösung $x = 12$, $y = 5$ zu.

II. In einer Rechnung findet sich der Posten

$$*24 \text{ ℔ à Mk. } 1{,}9* = \text{Mk. } *38{,}08\,.$$

Da wo das Zeichen * steht, sind die Ziffern unleserlich. Wie heissen diese Ziffern?

Werden dieselben der Reihe nach mit x, y, z bezeichnet, so erhält man, wenn man auf Pfennige rechnet, die Gleichung

$$(24 + 100x)(190 + y) = 3808 + 10\,000\,z\,,$$

und daraus folgt leicht

$$y = -190 + 4 \cdot \frac{238 + 625z}{25x + 6}\,.$$

Nun soll y eine der Zahlen 0, 1, 2, ..., 9 sein, daher muss

$$4 \cdot \frac{238 + 625z}{25x + 6} < 200, \text{ aber } > 190, \text{ also}$$

$$\frac{238 + 625z}{25x + 6} < 50, \quad \text{aber} \quad > 48$$

sein. Dieser Bruch kann also die Werthe 49 und 48 haben. Nun folgt aber aus der Annahme

$$\frac{238 + 625z}{25x + 6} = 49\,,$$

dass

$238 + 625z = 1225x + 294$, also $625z \equiv 56 \pmod{1225}$ sein müsste, und diese Congruenz ist nach § 21, Lehrsatz II unmöglich. Wird weiter

$$\frac{238 + 625z}{25x + 6} = 48$$

gesetzt, so ergiebt sich der Reihe nach

$$\begin{aligned} 238 + 625z &= 1200x + 288, \\ 625z &= 1200x + 50, \\ 25z &= 48x + 2, \\ 48x &\equiv -2 \pmod{25}, \\ -2x &\equiv -2 \pmod{25}, \\ x &\equiv 1 \pmod{25}, \\ x &= 1 + 25k, \end{aligned}$$

wo k noch unbestimmt bleibt. Setzt man diesen Werth von x in die Gleichung

$$25z = 48x + 2,$$

so erhält man

$$z = 2 + 48k.$$

Endlich ist noch $y = -190 + 4 \cdot 48 = 2$. Damit x und z einstellig seien, ist $k = 0$ anzunehmen; also erhalten wir die eine Lösung

$$x = 1, \quad y = 2, \quad z = 2.$$

III. Die Zahlen zu bestimmen, die für gegebene Moduln $m_1, m_2, \ldots$ gegebene Reste $r_1, r_2, \ldots$ geben.

Die gesuchten Zahlen x sollen den Congruenzen

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \ldots,$$

d. h. den Gleichungen

$$\begin{aligned} x &= r_1 + m_1 y, \\ x &= r_2 + m_2 z, \\ &\ldots\ldots \end{aligned}$$

genügen, wo $y, z, \ldots$ unbestimmte Zahlen sind. Setzt man den in der ersten Gleichung angegebenen Werth von x in die zweite Gleichung ein, so werden y und z, folglich auch x (nöthigenfalls mittels einer neuen Unbestimmten) bestimmt. Der so erhaltene Werth von x wird in die dritte Gleichung eingesetzt und durch Auflösung derselben ein neuer Ausdruck

für x hergeleitet. So gelangt man nach und nach zu dem Ausdruck von x, welcher allen gegebenen Bedingungen genügt.

1. Beispiel. Welche Zahl giebt, durch 5 dividirt, 2, und durch 6 dividirt, 5 zum Rest?

Die gesuchte Zahl x muss die Form $5y + 2$ haben und zugleich für den Modul 6 kongruent 5 sein. Es ist also

$$5y + 2 \equiv 5 \pmod{6}, \quad 5y \equiv 3 \pmod{6}.$$

Hieraus ergiebt sich $y \equiv 3 \pmod{6}$, also ist

$$y = 3 + 6k, \quad x = 5(3 + 6k) + 2 = 17 + 30k,$$

wo k jede ganze Zahl sein kann.

2. Beispiel. (Aus einer alten chinesischen Arithmetik). Es wird angezeigt, dass drei Reisfässer, deren jedes gleichviel Reis enthält, von Dieben zum Theil geleert worden sind. Man wusste nicht, wie viel Reis sich im Ganzen darin befand, jedoch weniger als 1000 Ho (kleines chinesisches Maass), aber es ergab sich, dass in dem einen Fasse noch 1 Ho übrig gelassen war, in dem zweiten noch 11 Ho und in dem dritten noch 1 Ho. Als man der Diebe habhaft wurde, gestand A, dass er mit einer Schaufel mehrere Male aus dem ersten Fasse den Reis in einen Sack gefüllt habe; B, dass er in der Eile einen hölzernen Schuh ergriffen und diesen mehrere Male aus dem zweiten Fasse voll geschüttet; C, dass er eine Schüssel mehrere Male aus dem dritten Fasse gefüllt habe. Diese drei Gefässe, deren sich die Diebe bedient haben, sind zur Stelle, und es ergiebt sich, dass die Schaufel 11 Ho, der Holzschuh 17 Ho und die Schüssel 12 Ho enthält. Wie viel Reis befand sich in jedem Fasse?

A habe y mal den Inhalt der Schaufel, also $11y$ Ho gestohlen, so ergiebt sich für den Inhalt x des ersten Fasses $11y + 1$. Ebenso liefern die Geständnisse des B und des C für dieselbe Grösse die Ausdrücke $17z + 11$, $12u + 1$, so dass wir die drei Gleichungen

$$x = 11y + 1, \quad x = 17z + 11, \quad x = 12u + 1$$

erhalten. Es ist daher zunächst

$$11y + 1 = 17z + 11,$$

also

$$17z \equiv -10 \pmod{11},$$

und hieraus folgt der Reihe nach

$$6z \equiv -10, \quad 3z \equiv -5 \equiv 6, \quad z \equiv 2 \pmod{11},$$

$$z = 2 + 11k, \quad x = 45 + 187k,$$

wo k eine ganze Zahl bedeutet.

Wird dieser Werth von x in die dritte Gleichung eingesetzt, so erhält man

$$45 + 187k = 12u + 1,$$

also

$$187k \equiv -44 \pmod{12}, \quad 7k \equiv 4 \pmod{12}$$

und hieraus

$$k \equiv 4 \pmod{12}, \quad \text{oder} \quad k = 4 + 12k',$$

wo k' gleichfalls eine noch unbestimmte ganze Zahl bezeichnet. Es ist also

$$x = 45 + 187(4 + 12k') = 793 + 2244k',$$

und da $x < 1000$ sein soll, so ist $k' = 0$ anzunehmen, also

$$x = 793.$$

IV. Einen Bruch $\frac{Z}{N}$ in Partialbrüche zu zerlegen, deren Nenner die Factoren von N sind.

Ist $N = a \,.\, b \,.\, c \ldots k$, wo $a, b, c, \ldots, k$ prim zu einander sind, so setzen wir

$$\frac{Z}{N} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \cdots + \frac{\varkappa}{k}$$

und erhalten durch Multiplication mit N

$$Z = \alpha \,.\, bc \ldots k + \beta \,.\, ac \ldots k + \cdots$$

Da nun alle Glieder mit Ausnahme von Z und

$$\alpha \,.\, bc \ldots k$$

durch a theilbar sind, so muss

$$Z \equiv \alpha \,.\, bc \ldots k \pmod{a}$$

sein. Ebenso ergeben sich weiter die Bedingungen

$$Z \equiv \beta \,.\, ac \ldots k \pmod{b},$$

$$Z \equiv \gamma \,.\, abd \ldots k \pmod{c},$$

$$\cdots\cdots\cdots\cdots$$

Jede dieser Congruenzen liefert den Werth einer der Unbekannten $\alpha, \beta, \ldots \varkappa$.

Beispiel. Um den Bruch $\frac{49}{60}$ in seine Partialbrüche zu zerlegen, setzen wir

$$\frac{49}{60} = \frac{\alpha}{3} + \frac{\beta}{4} + \frac{\gamma}{5}$$

und erhalten durch Multiplication mit 60

$$49 = 4 \,.\, 5 \,.\, \alpha + 3 \,.\, 5 \,.\, \beta + 3 \,.\, 4 \,.\, \gamma,$$

also die drei Congruenzen

$$49 \equiv 20\alpha \ (\text{mod.}\ 3), \qquad 49 \equiv 15\beta \ (\text{mod.}\ 4),$$
$$49 \equiv 12\gamma \ (\text{mod.}\ 5),$$

oder vereinfacht

$$2\alpha \equiv 1 \ (\text{mod.}\ 3), \quad 3\beta \equiv 1 \ (\text{mod.}\ 4), \quad 2\gamma \equiv 4 \ (\text{mod.}\ 5).$$

Die Wurzeln dieser Congruenzen sind

$$\alpha \equiv 2 \ (\text{mod.}\ 3), \quad \beta \equiv 3 \ (\text{mod.}\ 4), \quad \gamma \equiv 2 \ (\text{mod.}\ 5).$$

Es ist also, wenn k, k', k'' unbestimmte ganze Zahlen bezeichnen,

$$\alpha = 2 + 3k, \quad \beta = 3 + 4k', \quad \gamma = 2 + 5k'',$$

und durch Einsetzung dieser Werthe in die gegebene Gleichung erhält man

$$49 = (40 + 60k) + (45 + 60k') + (24 + 60k'')$$

oder

$$49 = 109 + 60\,(k + k' + k'').$$

Wir haben danach über k, k', k'' so zu verfügen, dass

$$k + k' + k'' = -1$$

werde. Das ist auf unendlich viele Arten möglich. Fügen wir aber die Bedingung hinzu, dass die Partialbrüche e c h t e Brüche sein sollen, so erhalten wir nur d r e i Werthsysteme für k, k', k'', nämlich

$$k = 0, \qquad k' = 0, \qquad k'' = -1,$$
$$k = 0, \qquad k' = -1, \quad k'' = 0,$$
$$k = -1, \quad k' = 0, \qquad k'' = 0,$$

welchen die Lösungen

$$\frac{49}{60} = \frac{2}{3} + \frac{3}{4} - \frac{3}{5},$$
$$\frac{49}{60} = \frac{2}{3} - \frac{1}{4} + \frac{2}{5},$$
$$\frac{49}{60} = -\frac{1}{3} + \frac{3}{4} + \frac{2}{5}$$

entsprechen.

V. Es seien m und n zwei relative Primzahlen. Man soll zwei ganze Zahlen x, y bestimmen, für welche die Gleichung

(1) $$mx + ny = 1$$

besteht.

Die Gleichung ist der Congruenz

(2) $$mx \equiv 1 \pmod{n}$$

äquivalent. Da m prim zu n ist, so hat diese Congruenz **eine** Wurzel $x = \xi + kn$, durch deren Einsetzung in (1) sich ein Ausdruck $y = \eta - mk$ ergiebt. Da k jede ganze Zahl sein kann, so hat die vorgelegte Gleichung (1) unendlich viele Lösungen.

Beispiel. $3x + 4y = 1$.

Die Congruenz $3x \equiv 1 \pmod{4}$ hat die Wurzel $x \equiv 3 \pmod{4}$. Setzt man in die vorgelegte Gleichung $x = 3 + 4k$, so ergiebt sich $y = -2 - 3k$, und man erhält für x und y, je nach dem Werthe, den man k beilegt,

k	..	-2	-1	0	$+1$	$+2$	..
x	..	-5	-1	3	7	11	..
y	..	4	1	-2	-5	-8	..

VI. Es seien $A, B, C, D, \ldots$ gegebene ganze Zahlen, deren grösster gemeinschaftlicher Divisor $= \mu$ ist. Man soll ganze Zahlen $a, b, c, d, \ldots$ so bestimmen, dass die Gleichung

$$aA + bB + cC + \cdots = \mu$$

besteht.

Lösung. Wenn zunächst die beiden ersten Zahlen A, B den grössten gemeinschaftlichen Divisor d_1 haben, so können wir die Gleichung

$$Ax + By = d_1$$

oder die Congruenz

$$Ax \equiv d_1 \pmod{B}$$

lösen. Hat letztere die Wurzel α, so ist

$$A\alpha = d_1 - \beta B,$$

also

$$A\alpha + B\beta = d_1,$$

wo α, β ganze Zahlen sind.

Ebenso können wir weiter, wenn d_1 und die dritte Zahl den grössten gemeinschaftlichen Divisor d_2 haben, zwei ganze Zahlen γ, δ so bestimmen, dass

$$\gamma d_1 + \delta C = d_2,$$

d. h.

$$\gamma\alpha A + \gamma\beta B + \delta C = d_2$$

wird, und man erkennt leicht, dass d_2 der grösste gemeinschaftliche Divisor von A, B, C sein muss. Als grösster gemeinschaftlicher Divisor von d_1 und C muss nämlich d_2 in jede der Zahlen A, B, C aufgehen. Wäre nun nicht d_2, sondern $d'_2 > d_2$ der grösste gemeinschaftliche Divisor von A, B, C, so würde wegen der letzten Gleichung d'_2 in d_2 aufgehen müssen, die grössere Zahl also ein Divisor einer kleineren sein. Demnach ist in der That d_2 der grösste gemeinschaftliche Divisor von A, B, C.

Wenn noch eine vierte Zahl D vorhanden ist, so nehmen wir weiter den grössten gemeinschaftlichen Divisor d_3 von d_2 und D (der dann der grösste gemeinschaftliche Divisor von A, B, C, D sein wird) und lösen die Gleichung $\varepsilon d_2 + \eta D = d_3$; dann ist

$$\gamma\alpha\varepsilon A + \gamma\beta\varepsilon B + \delta\varepsilon C + \eta D = d_3.$$

So fortfahrend gelangt man schliesslich zur Lösung der gestellten Aufgabe.

I. Beispiel. $14x + 18y + 9z = 1.$

$14\alpha + 18\beta = 2$ hat die Lösung $\alpha = 4$, $\beta = -3$,
$2\gamma + 9\delta = 1$ „ „ „ $\gamma = -4$, $\delta = 1$,

also ist

$$[14 \cdot 4 + 18 \cdot (-3)](-4) + 9 \cdot 1 = 1,$$

d. h.

$$x = -16,\ y = +12,\ z = +1.$$

II. Beispiel. $3x + 6y + 8z + 12u = 1.$

$3\alpha + 6\beta = 3$ hat die Lösung $\alpha = -1$, $\beta = 1$
$3\gamma + 8\delta = 1$ „ „ „ $\gamma = 3$, $\delta = -1$
$\varepsilon + 12\eta = 1$ „ „ „ $\varepsilon = 13$, $\eta = -1$,

also ist

$$x = \alpha\gamma\varepsilon = -39,\ y = \beta\gamma\varepsilon = 39,\ z = \delta\varepsilon = -13,\ u = \eta = -1.$$

§ 25. Auflösung einer Congruenz ersten Grades mit mehreren Unbekannten. — Die Congruenz

$$ax + by + cz + \cdots \equiv r \pmod{m}$$

ist offenbar nur dann möglich, wenn der grösste gemeinschaftliche Divisor d der Zahlen $a, b, c, \ldots$ und m auch in r aufgeht. Wenn dies der Fall ist, so fällt d durch Division weg. Wir setzen daher von vornherein $d = 1$ voraus. Die gegebene Congruenz ist nun gleichbedeutend mit der unbestimmten Gleichung

$$ax + by + cz + \cdots = r + mk,$$

und diese lösen wir für die Unbekannte, welche den kleinsten Coefficienten hat.

Das Verfahren stimmt mit dem in § 22 dargelegten ganz überein, und die Unbekannten werden mittels so vieler unbestimmten Grössen ausgedrückt, als in der gegebenen Congruenz Unbekannte vorhanden sind. Besondere Sorgfalt hat man anzuwenden, wenn man alle Lösungen ermitteln will, wie sich im folgenden Beispiel zeigen wird.

Beispiel. Ein Münzmeister hat dreierlei Silber; das erste ist 14-, das zweite 11-, das dritte 9löthig. Er braucht 30 Mark 12löthiges Silber. Wie viel ganze Mark muss er von jeder Sorte nehmen?

x Mark der ersten, y Mark der zweiten und z Mark der dritten Sorte sollen zusammen $30 . 12 = 360$ Loth Silber enthalten. Es muss also

$$(1) \qquad 14x + 11y + 9z = 360$$

oder

$$(2) \qquad 14x + 11y \equiv 360 \pmod{9}$$

sein. Diese Congruenz liefert der Reihe nach

$$-4x + 2y \equiv 0 \pmod{9}, \; -2x + y \equiv 0 \pmod{9}, \; y = 2x + 9k.$$

Wird dieser Werth von y in (1) eingesetzt, so folgt nach einigen Vereinfachungen

$$z = 40 - 4x - 11k.$$

x und k sind noch unbestimmt geblieben; x ist positiv anzunehmen, und k muss so gewählt werden, dass y, z positiv werden. Um nun **alle** Lösungen zu erhalten, suchen wir k

in Grenzen einzuschliessen. Die für y und z erhaltenen Ausdrücke liefern, wenn x eliminirt wird,

$$2y + z = 40 + 7k, \tag{3}$$

und aus dem Werthe von z folgt

$$z + 4x = 40 - 11k. \tag{4}$$

Da die linken Seiten der Gleichungen (3) und (4) positiv sind, so müssen es auch die rechten sein, d. h. k muss zwischen $-\frac{40}{7}$ und $+\frac{40}{11}$ liegen. k kann also die 9 Werthe

$$-5, -4, -3, -2, -1, 0, 1, 2, 3$$

haben.

Ist nun erstens $k = -5$, so gehen die Ausdrücke von y und z über in

$$y = 2x - 45, \; z = -4x + 95;$$

damit y positiv sei, muss x wenigstens 23 sein, und damit z positiv sei, darf x nicht grösser als 23 sein. Dieser Fall liefert also die eine Lösung

$$x = 23, \; y = 1, \; z = 3.$$

Wenn zweitens $k = -4$ ist, so werden die Ausdrücke für y und z

$$y = 2x - 36, \; z = 84 - 4x,$$

und damit diese positive und von Null verschiedene Werthe haben, muss $x > 18$ und < 21 sein. x ist also entweder 19 oder 20, so dass wir die beiden Lösungen

$$x = 19, \; y = 2, \; z = 8$$
$$x = 20, \; y = 4, \; z = 4$$

erhalten.

Ist drittens $k = -3$, so erhalten wir

$$y = 2x - 27, \; z = 73 - 4x$$

und erkennen, dass $x > 13$ und < 19 sein muss, also eine der 5 Zahlen 14, 15, ..., 18 sein kann. Dadurch ergeben sich die 5 Lösungen

$$x = 14, \; y = 1, \; z = 17$$
$$x = 15, \; y = 3, \; z = 13$$
$$x = 16, \; y = 5, \; z = 9$$
$$x = 17, \; y = 7, \; z = 5$$
$$x = 18, \; y = 9, \; z = 1.$$

Auf diese Weise erhalten wir für $k = -2$ noch 6, für $k = -1$ noch 8, für $k = 0$ noch 9, für $k = 1$ noch 7, für $k = 2$ noch 4, endlich für $k = 3$ noch 1 Lösung, so dass die Aufgabe auf 43 verschiedene Arten gelöst werden kann.

§ 26. Auflösung eines Systems von m Congruenzen ersten Grades mit m oder mehr Unbekannten. — Liegen m auf denselben Modul bezügliche Congruenzen ersten Grades mit $m + n$ Unbekannten vor (wo n auch $= 0$ sein kann), so leitet man durch Elimination ein neues System her, in welchem jede folgende Congruenz eine Unbekannte weniger als die vorhergehende enthält, so dass sich in der letzten noch $n + 1$ Unbekannte befinden. Setzt man die durch Auflösung dieser letzten Congruenz gefundenen Werthe der $n + 1$ Unbekannten in die vorhergehenden Congruenzen ein, so werden auch die übrigen Unbekannten der Reihe nach bestimmt.

Beispiel. Es sei das System

$$\left.\begin{aligned} 4x - 3y + 7z &\equiv 5 \\ 5x + y - 3z &\equiv 2 \\ x - 4y - z &\equiv 1 \end{aligned}\right\} \pmod{14}$$

gegeben. Wird der aus der dritten Congruenz genommene Werth von x

$$x \equiv 1 + 4y + z \pmod{14}$$

in die beiden ersten eingesetzt, so ergiebt sich

$$\left.\begin{aligned} -y - 3z &\equiv 1 \\ 7y + 2z &\equiv -3 \end{aligned}\right\} \pmod{14}.$$

Weiter liefert die erste dieser beiden Congruenzen

$$y \equiv -1 - 3z \pmod{14},$$

und dieser Werth reducirt die zweite auf

$$5z \equiv -4 \pmod{14}.$$

Das neue System, das wir aus dem gegebenen hergeleitet haben, ist also

$$\left.\begin{aligned} x &\equiv 1 + 4y + z \\ y &\equiv -1 - 3z \\ 5z &\equiv -4 \end{aligned}\right\} \pmod{14}.$$

Die letzte Congruenz, für welche wir auch

$$5z \equiv 10 \pmod{14}$$

schreiben können, hat die Wurzel $z \equiv 2$; die zweite Congruenz liefert sodann $y \equiv -7 \equiv +7$ und die erste $x \equiv 3 \pmod{14}$.

Wenn die gegebenen m Congruenzen sich auf verschiedene Moduln beziehen, so hat man jede durch die entsprechende unbestimmte Gleichung zu ersetzen, wodurch m neue Unbekannte eingeführt werden, und durch Elimination eine Gleichung zu bilden, welche $m-1$ der Unbekannten nicht mehr enthält. Mit dieser Gleichung ist dann auf die in § 22 angegebene Weise zu verfahren. Ebenso behandelt man Aufgaben, die von vorn herein zu m linearen Gleichungen mit mehr als m Unbekannten führen.

Beispiel. Aus den Gleichungen

$$x + 3y + 5z = 44$$
$$3x + 5y + 7z = 68$$

folgt durch Elimination von x

$$4y + 8z = 64.$$

Diese Gleichung liefert für y den Werth

$$y = 16 - 2z,$$

nach dessen Einsetzung in die erste Gleichung man für x den Werth

$$x = z - 4$$

erhält. z ist unbestimmt, muss aber, damit y positiv sei, < 8, und damit x positiv sei, > 4 angenommen werden. Wir erhalten somit drei Lösungen

$$x = 1,\ y = 6,\ z = 5$$
$$x = 2,\ y = 4,\ z = 6$$
$$x = 3,\ y = 2,\ z = 7.$$

§ 27. **Auflösung der unbestimmten Gleichung zweiten Grades mit zwei Unbekannten, von denen die eine nur im ersten Grade vorkommt.** — Es soll die Gleichung

$$ax + by + cxy + dy^2 + f = 0,$$

deren Coefficienten a, b, c, d, f ganze Zahlen sind, in ganzen Zahlen aufgelöst werden. Zunächst ergiebt sich

$$x = -\frac{dy^2 + by + f}{cy + a}.$$

Diese Division wollen wir ausführen, vorher aber dafür Sorge tragen, dass die Coefficienten des Quotienten ganze Zahlen werden. Zu diesem Zwecke haben wir uns nöthigenfalls nicht mit dem Ausdruck von x, sondern mit

$$c^2 x = -\frac{c^2 d y^2 + b c^2 y + c^2 f}{c y + a}$$

zu beschäftigen. Es ergiebt sich

$$x, \text{ resp. } c^2 x = \alpha y + \beta + \frac{\gamma}{c y + a},$$

wo α, β, γ ganze Zahlen sind. Damit nun x, resp. $c^2 x$ eine ganze Zahl werde, muss man y einen solchen Werth beilegen, dass $cy + a$ in γ aufgehe; mit anderen Worten, $cy + a$ muss ein Divisor von γ sein. Man wähle also von den Divisoren von γ diejenigen aus, welche, um a vermindert, durch c theilbar werden. Jeder dieser Divisoren liefert einen Werth von y und weiter einen ganzzahligen Werth von $c^2 x$; von den so erhaltenen Werthen sind natürlich nur diejenigen zu nehmen, für welche auch x eine ganze Zahl wird.

Beispiel. Aus der Gleichung

$$3x + 5xy + 2y - 3y^2 = 15$$

folgt

$$x = \frac{3y^2 - 2y + 15}{5y + 3}$$

oder

$$25x = \frac{75y^2 - 50y + 375}{5y + 3} = 15y - 19 + \frac{432}{5y + 3}.$$

Von den 20 Divisoren der Zahl $432 = 2^4 \cdot 3^3$ sind nur die zu benutzen, welche, um 3 verringert, durch 5 theilbar werden, also, wenn wir uns auf positive Werthe der Unbekannten beschränken, 8, 18, 48, 108. Wird $5y + 3$ der Reihe nach jeder dieser Zahlen gleichgesetzt, so erhält man vier Werthe von y, zu deren jedem ein Werth von x gehört, nämlich

$$\left.\begin{matrix} y = 1 \\ x = 2 \end{matrix}\right\}, \quad \left.\begin{matrix} y = 3 \\ x = 2 \end{matrix}\right\}, \quad \left.\begin{matrix} y = 9 \\ x = 5 \end{matrix}\right\}, \quad \left.\begin{matrix} y = 21 \\ x = 12 \end{matrix}\right\}.$$

Diese Methode hört auf, anwendbar zu sein, wenn $c = 0$, also

$$x = -\frac{d y^2 + b y + f}{a}$$

ist. Bezeichnet dann η eine ganze Zahl, die, für y eingesetzt,

x zu einer ganzen Zahl macht, so wird auch $\eta + ka$, wo k eine beliebige positive oder negative ganze Zahl bezeichnet, dieser Bedingung genügen, da

$$d(\eta + ka)^2 + b(\eta + ka) + f$$
$$= (d\eta^2 + b\eta + f) + a(2dk\eta + adk^2 + bk)$$

ist. Wenn $\eta > \frac{a}{2}$ ist, so kann man offenbar über die Grösse und das Vorzeichen von k so verfügen, dass der absolute Werth von $\eta + ka < \frac{a}{2}$ werde. Durch Einsetzen der Zahlen 1, 2, ... bis zu der grössten ganzen Zahl, die nicht grösser als $\frac{a}{2}$ ist, in den Ausdruck für x wird man also die Werthe von y ermitteln, die x zu einer ganzen Zahl machen.

Beispiel. Aus

$$5x - 6y + 3y^2 - 464 = 0$$

folgt

$$x = \frac{-3y^2 + 6y + 464}{5} = y + 92 + \frac{-3y^2 + y + 4}{5}.$$

Der Ausdruck $-3y^2 + y + 4$ soll durch 5 theilbar sein. Um die Werthe von y zu ermitteln, die dies bewirken, haben wir in denselben nur die Zahlen -2, -1, 1, 2 einzusetzen. Für diese Werthe von y nimmt derselbe beziehungsweise die Werthe -10, 0, 2, -6 an. Es sind also $-2 + 5k$ und $-1 + 5k'$ die gesuchten Werthe von y, und darin bezeichnen k, k' beliebige ganze Zahlen. Die zugehörigen Werthe von x sind

$$+88 + 18k - 15k^2 \quad \text{und} \quad 91 + 12k' - 15k'^2.$$

Will man sich auf positive Werthe beschränken, so liefert das erste Paar der Ausdrücke für x und y die drei Lösungen

$$x = 91, \quad y = 3,$$
$$x = 64, \quad y = 8,$$
$$x = 7, \quad y = 13,$$

das zweite Paar die beiden Lösungen

$$x = 88, \quad y = 4,$$
$$x = 55, \quad y = 9.$$

Anmerkung. Ueber die Ausdehnung dieser Methode auf Gleichungen höherer Grade mit zwei Unbekannten, von denen die eine nur im ersten Grade vorkommt, s. Lagrange's Zusatz III zu Euler's Algebra.

§ 28. Ermittlung der rationalen (ganzen oder gebrochenen) Werthe von x, für welche der Ausdruck

$$a + bx + cx^2$$

ein vollständiges Quadrat wird. — Diese Aufgabe ist nur ein specieller Fall der allgemeineren: Die unbestimmte Gleichung zweiten Grades mit zwei Unbekannten in rationalen Zahlen zu lösen. Diese letztere Aufgabe wird weiter unten behandelt werden. Hier soll der Ausdruck $a + bx + cx^2$ nicht allgemein (für beliebige Werthe der Coefficienten a, b, c) in ein Quadrat verwandelt werden, sondern unter gewissen Voraussetzungen, die die Sache ungemein vereinfachen und immer ermöglichen. Ist nämlich

1) a ein Quadrat $= \alpha^2$, so können wir

$$a + bx + cx^2 = (\alpha + kx)^2 = \alpha^2 + 2\alpha kx + k^2x^2$$

setzen, wo k eine unbestimmte Zahl bezeichnet, und erhalten leicht

$$x = \frac{b - 2\alpha k}{k^2 - c}.$$

Danach ist z. B. $4 + 5x + 6x^2$ ein Quadrat, wenn man

$$x = \frac{5 - 4k}{k^2 - 6}$$

annimmt, wo k jede rationale Zahl sein kann. Für $k = 1$ ist $x = -\frac{1}{5}$, und in der That ist

$$4 - 1 + \frac{6}{25} = \frac{81}{25} = \left(\frac{9}{5}\right)^2.$$

2) Es sei c ein Quadrat $= \gamma^2$; dann setzen wir

$$a + bx + \gamma^2x^2 = (k + \gamma x)^2,$$

wo k eine unbestimmte rationale Zahl bedeutet. Es ergiebt sich

$$x = \frac{a - k^2}{2\gamma k - b}.$$

Danach ist z. B. $7 + 3x + 25x^2$ ein Quadrat, wenn man

$$x = \frac{7 - k^2}{10k - 3}$$

annimmt. Für $k = 0, -1, +1, \frac{1}{2}$ ist beziehungsweise

$$x = -\frac{7}{3}, \; -\frac{6}{13}, \; \frac{6}{7}, \; \frac{27}{8}.$$

3) Die Aufgabe ist ferner sehr leicht zu lösen, wenn $a + bx + cx^2$ sich in zwei Factoren ersten Grades mit rationalen Coefficienten zerlegen lässt. Das ist der Fall, wenn

$$b^2 - 4ac \text{ ein Quadrat } = h^2$$

ist; denn unter dieser Voraussetzung hat die Gleichung

$$a + bx + cx^2 = 0$$

die Wurzeln $\frac{-b \pm h}{2c}$, so dass

$$a + bx + cx^2 = c\left(x - \frac{h-b}{2c}\right)\left(x + \frac{h+b}{2c}\right)$$

ist.

Wir nehmen also an, es sei

$$a + bx + cx^2 = (d + ex)(f + gx),$$

und setzen

$$(d + ex)(f + gx) = \frac{m^2(d + ex)^2}{n^2};$$

dann erhalten wir

$$x = \frac{dm^2 - fn^2}{gn^2 - em^2}.$$

So z. B. ist $56x^2 + 19x - 15 = (7x + 5)(8x - 3)$, und wenn wir

$$56x^2 + 19x - 15 = (7x + 5)(8x - 3) = \frac{m^2}{n^2}(7x + 5)^2$$

setzen, so ergibt sich

$$x = \frac{5m^2 + 3n^2}{-7m^2 + 8n^2},$$

also etwa für $m = 1$, $n = 1$

$$x = 8.$$

4) Endlich lassen sich leicht Werthe von x bestimmen, für welche $a + bx + cx^2$ ein Quadrat wird, wenn sich dieser Ausdruck auf die Form $p^2 + q \cdot r$ bringen lässt, wo p, q, r Functionen ersten Grades von x (mit rationalen Coefficienten) sind. Setzt man nämlich

$$a + bx + cx^2 = p^2 + qr = \left(p + \frac{m}{n}q\right)^2,$$

so ergiebt sich

$$r = \frac{2mp}{n} + \frac{m^2 q}{n^2},$$

und aus dieser Gleichung ersten Grades lässt sich x leicht bestimmen.

Es ist z. B.

$$7x^2 + 2 = 9x^2 - 2(x^2 - 1) = (3x)^2 - (2x - 2)(x + 1),$$

also

$$p = 3x, \quad q = -2x + 2, \quad r = x + 1,$$

und daraus erhält man leicht

$$x = \frac{2m^2 - n^2}{2m^2 - 6mn + n^2},$$

also etwa für $m = 1$, $n = 1$

$$x = -\frac{1}{3}.$$

§ 29. Auflösung der Pythagoreischen Gleichung in ganzen Zahlen (Euklids Elemente, X, 29). — Um die Gleichung

$$x^2 + y^2 = z^2$$

in ganzen Zahlen aufzulösen, setze man

$$\frac{x}{z} = u, \quad \frac{y}{z} = v;$$

dann ist

$$u^2 + v^2 = 1;$$

also wird $u = 1 - kv$ sein, wo k eine vorläufig unbestimmte Zahl bezeichnet. Für diesen Werth von u geht die zu lösende Gleichung über in

$$(1 - kv)^2 + v^2 = 1,$$

woraus sich leicht

$$v = \frac{2k}{1 + k^2}, \quad 1 - kv = \frac{1 - k^2}{1 + k^2}$$

ergiebt. In der That ist

$$\left(\frac{2k}{1 + k^2}\right)^2 + \left(\frac{1 - k^2}{1 + k^2}\right)^2 = 1,$$

also auch

$$(2k)^2 + (1 - k^2)^2 = (1 + k^2)^2.$$

Diese Identität löst die gegebene Aufgabe; denn es ist

$$x = \pm 2k, \quad y = \pm (1 - k^2), \quad z = \pm (1 + k^2),$$

wo k jede ganze Zahl sein kann. So z. B. ist für

k	x	y	z
2	4	3	5
3	6	8	10
4	8	15	17
5	10	24	26
6	12	35	37
. .	. .	. .	. .

Anmerkung. Eine der Zahlen x, y ist durch 3, eine derselben durch 4, und eine der Zahlen x, y, z ist durch 5, also das Produkt xyz durch 60 theilbar.

Beweis. Da eine von drei auf einander folgenden Zahlen durch 3 theilbar und $y = (k - 1)(k + 1)$ ist, so muss die Zahl 3 entweder in $x = 2k$ oder in einen der Factoren von y aufgehen.

Wenn ferner k gerade ist, so ist x durch 4 theilbar. Ist dagegen $k = 2n + 1$, so ist $y = k^2 - 1 = 4n^2 + 4n$ durch 4 theilbar.

Endlich kann k für den Modul 5 die Reste 0, oder ± 1 oder ± 2 geben, also von der Form $5n$ oder $5n \pm 1$ oder $5n \pm 2$ sein. Im ersten Falle ist $x = 10n$, im zweiten $y = k^2 - 1 = 25n^2 \pm 10n$, im dritten $z = k^2 + 1 = 25n^2 \pm 20n + 5$ durch 5 theilbar.

§ 30. Der Wilson'sche Satz. — Die Theorie der Congruenzen ersten Grades liefert einen direkten Beweis des berühmten Wilson'schen Satzes:

Das um 1 vermehrte Produkt aller Zahlen von 1 bis $p - 1$, also die Zahl

$$z = 1 \cdot 2 \cdot 3 \cdots (p-1) + 1$$

ist durch p theilbar, wenn p eine Primzahl ist, sonst nicht.

Beweis. Es sei p eine Primzahl, und es bezeichne a irgend eine der Zahlen 1, 2, 3, ..., $(p - 1)$, so wird a prim zu p sein und die Congruenz $ax \equiv 1 \pmod{p}$ nach dem

Früheren stets eine, aber auch nur eine Wurzel haben. Wäre diese Wurzel gleich dem Coefficienten a, also $a^2 \equiv 1 \pmod{p}$, so müsste $a^2 - 1 = (a+1)(a-1)$ durch p theilbar sein, also p entweder in $a+1$ oder in $a-1$ aufgehen. Nun ist aber a kleiner als p. Ginge also p in $a+1$ auf, so müsste $a = p - 1$ sein, und ginge p in $a-1$ auf, so müsste $a - 1 = 0$, also $a = 1$ sein. Wenn daher a weder 1, noch $p - 1$, sondern eine der Zahlen $2, 3, 4, \ldots, (p-2)$ ist, so kann die Wurzel der Congruenz $ax \equiv 1 \pmod{p}$ nie gleich dem Coefficienten a sein. Ferner können zwei Congruenzen mit verschiedenen Coefficienten a, a'

$$ax \equiv 1, \quad a'x \equiv 1 \pmod{p}$$

nicht dieselbe Wurzel x haben; denn sonst würde man aus $ax \equiv a'x \pmod{p}$ durch Division mit x die Congruenz $a \equiv a' \pmod{p}$ erhalten, während zwei verschiedene Zahlen der Reihe $2, 3, \ldots, (p-2)$ für den Modul p nicht congruent sein können. Die Zahlen $2, 3, \ldots, (p-2)$ lassen sich somit in Gruppen von je zweien zusammenstellen, so dass das Produkt der Zahlen jeder Gruppe den Rest 1 liefert. Durch Multiplication aller so gebildeten Congruenzen erhält man

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

und hieraus folgt durch Multiplication mit $p - 1$

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv p - 1 \equiv -1 \pmod{p}$$

oder

$$1 \cdot 2 \cdot 3 \cdots (p-1) + 1 \equiv 0 \pmod{p},$$

was bewiesen werden sollte.

Wenn dagegen p keine Primzahl, sondern durch eine Zahl q, die also $< p$ ist, theilbar ist, so tritt q als Factor in dem Produkt $1 . 2 . 3 \ldots (p-1)$ auf. Die Zahl z ist also nicht durch q und somit auch nicht durch p theilbar.

Anmerkung. Dieser von seinem Entdecker nicht bewiesene Satz liefert eine allgemeine und untrügliche, aber wegen der ungeheuern Rechnung, die sie erfordert, in der Praxis gar nicht anzuwendende Regel, zu erkennen, ob eine gegebene Zahl eine Primzahl oder zusammengesetzt sei. Der obige Beweis ist von Gauss, Disquisitiones, 77 gegeben; andere Beweise sind von Lagrange, Abhandlungen der Berliner Akademie, 1771; Euler, Opuscula analytica I, p. 329; Legendre, theorie des nombres, II, 130; Stern, algebraische Analysis, p. 393.

§ 31. Der Fermat'sche Satz. — Bezeichnet a eine beliebige durch die Primzahl p nicht theilbare ganze Zahl, so ist

$$a^{p-1} \equiv 1 \pmod{p},$$

oder mit anderen Worten: die Congruenz

$$x^{p-1} \equiv 1 \pmod{p}$$

hat jede der $p-1$ Zahlen $1, 2, 3, \ldots, (p-1)$ zur Wurzel.

Beweis. Wir betrachten die Produkte, die man erhält, wenn man jede der Zahlen

$$(1) \qquad 1, 2, 3, \ldots, (p-1)$$

mit a multiplicirt, also die Zahlen

$$(2) \qquad a, 2a, 3a, \ldots, (p-1)a.$$

Die Reste dieser Produkte für den Modul p müssen sämmtlich von einander verschieden sein; denn aus der Annahme

$$ka \equiv k'a \pmod{p}$$

würde durch Division mit a sich

$$k \equiv k' \pmod{p}$$

ergeben, während zwei verschiedene Zahlen der Reihe (1), und als solche werden k und k' vorausgesetzt, nicht congruent sein können. Da nun ausserdem keins der Produkte (2) durch p theilbar ist, so müssen die Reste der Zahlen (2) in irgend einer Reihenfolge mit den Zahlen (1) übereinstimmen, und es muss folglich das Produkt aller Zahlen (2) dem Produkt aller Zahlen (1) congruent sein, d. h. es ist

$$1 \,.\, 2 \,.\, 3 \ldots (p-1)\, a^{p-1} \equiv 1 \,.\, 2 \,.\, 3 \ldots (p-1) \pmod{p},$$

und hieraus folgt durch Division mit $1 \,.\, 2 \,.\, 3 \ldots (p-1)$

$$a^{p-1} \equiv 1 \pmod{p}.$$

Anmerkung. Auch von diesem Satze, der von seinem Entdecker Fermat ohne Beweis in einem Briefe mitgetheilt worden ist (Varia opera mathematica, p. 163), giebt es mehrere Beweise (von Euler, Lambert, Gauss), die wir zum Theil noch kennen lernen werden.

§ 32. Ueber die Anzahl der Wurzeln einer Congruenz, deren Modul eine Primzahl ist.

Lehrsatz I. Eine nicht identische Congruenz, deren

Modul eine Primzahl ist, besitzt höchstens so viele Wurzeln, als ihr Grad Einheiten enthält.

Beweis. Wir nehmen an, die Congruenz

(1) $$Ax^m + Bx^{m-1} + \cdots + Mx + N \equiv 0 \pmod{p},$$

deren Coefficienten $A, B, \ldots, N$ ganze Zahlen sind, die wir nach dem Früheren als zwischen 0 und p oder auch zwischen $-\frac{p}{2}$ und $+\frac{p}{2}$ liegend voraussetzen dürfen, besitze mehr als m, also wenigstens $m+1$ Wurzeln $\alpha, \beta, \gamma, \ldots$ Die kleinste dieser Wurzeln sei α. Setzen wir dann $y+\alpha$ an die Stelle von x, so erhalten wir eine neue Congruenz m^{ten} Grades

(2) $$ay^m + by^{m-1} + \cdots + my + n \equiv 0 \pmod{p},$$

welche ebenso viele Wurzeln, wie die gegebene hat, indem sie durch die Werthe $0, \beta-\alpha, \gamma-\alpha, \ldots$ von y befriedigt wird. Da (2) die Wurzel $y = 0$ hat, so muss $n \equiv 0 \pmod{p}$ sein. Die Congruenz (2) lässt sich also auf die Form

(3) $$y(ay^{m-1} + by^{m-2} + \cdots + m) \equiv 0 \pmod{p}$$

bringen. Die linke Seite von (3) wird durch p theilbar, wenn man für y irgend eine der Grössen $\beta-\alpha, \gamma-\alpha, \ldots$ setzt, und da jede der letzteren prim zu p ist, so muss in allen diesen Fällen der Factor

$$ay^{m-1} + by^{m-2} + \cdots + m$$

durch p theilbar werden, d. h. die Congruenz

(4) $$ay^{m-1} + by^{m-2} + \cdots + m \equiv 0 \pmod{p}$$

muss die Wurzeln $\beta-\alpha, \gamma-\alpha, \ldots$ haben, deren Anzahl wenigstens gleich m ist.

Wenn es also eine Congruenz m^{ten} Grades mit mehr als m Wurzeln giebt, so lässt sich daraus eine Congruenz vom Grade $m-1$ mit mehr als $m-1$ Wurzeln, daraus ebenso eine Congruenz vom Grade $m-2$ mit mehr als $m-2$ Wurzeln, u. s. w., endlich eine Congruenz ersten Grades mit mehr als einer Wurzel herleiten, was dem Lehrsatz I des § 21 widerspricht.

Lehrsatz II. — Es seien $f(x)$ und $F(x)$ ganze Functionen von x, deren Coefficienten ganze Zahlen und deren Grade kleiner als die Primzahl p sind. Wenn

dann $f(x)$ ein Divisor von $x^{p-1} - 1 + pF(x)$ ist, so besitzt die Congruenz

$$f(x) \equiv 0 \pmod{p}$$

genau so viele Wurzeln, als ihr Grad Einheiten enthält.

Beweis. Da $f(x)$ ein Divisor von $x^{p-1} - 1 + pF(x)$ ist, so können wir

$$x^{p-1} - 1 + pF(x) = f(x)\,\varphi(x)$$

setzen, wo $\varphi(x)$ eine ganze Function von x mit ganzen Coefficienten bezeichnet. Nun ist nach dem Fermat'schen Satze $x^{p-1} - 1$ für jeden der $p-1$ Werthe $1, 2, \ldots, (p-1)$ von x durch p theilbar, und da $pF(x) \equiv 0 \pmod{p}$ eine identische Congruenz ist, so hat die Congruenz

$$f(x)\varphi(x) \equiv 0 \pmod{p},$$

deren linke Seite vom Grade $p-1$ ist, die $p-1$ Wurzeln $1, 2, 3, \ldots, (p-1)$. Hätte nun die Congruenz

$$f(x) \equiv 0 \pmod{p}$$

weniger Wurzeln, als ihr Grad Einheiten enthält, so würde

$$\varphi(x) \equiv 0 \pmod{p}$$

mehr Wurzeln haben müssen, als ihr Grad Einheiten enthält, und das widerspricht dem vorhergehenden Satze.

Lehrsatz III. — Wenn die Functionen $f(x)$ und $\varphi(x)$ einen grössten gemeinschaftlichen Divisor $\psi(x)$ haben, so sind die den Congruenzen

(1) $\qquad f(x) \equiv 0 \quad \text{und} \quad \varphi(x) \equiv 0 \pmod{p}$

gemeinschaftlichen Wurzeln auch Wurzeln der Congruenz

$$\psi(x) \equiv 0 \pmod{p}.$$

Beweis. Bezeichnen wir den Quotienten und den Rest der Division von $f(x)$ durch $\varphi(x)$ beziehungsweise mit Q und R, so ist

$$f(x) = Q\,.\,\varphi(x) + R,$$

und da danach für jede den Congruenzen (1) gemeinschaftliche Wurzel auch R durch p theilbar werden muss, so haben die Congruenzen (1) die nämlichen gemeinschaftlichen Wurzeln wie die Congruenzen

(2) $$\varphi(x) \equiv 0, \quad R \equiv 0 \pmod{p}.$$

Durch Fortsetzung dieser Schlüsse beweist man die Richtigkeit des vorliegenden Satzes.

Aufgabe. Die Zahl der Wurzeln einer Congruenz

(1) $$f(x) \equiv 0 \pmod{p},$$

wo p eine Primzahl ist, zu bestimmen.

Lösung. Da die Congruenz

(2) $$x^{p-1} - 1 \equiv 0 \pmod{p}$$

durch jede der $p-1$ Zahlen $1, 2, 3, \ldots (p-1)$ befriedigt wird, so haben wir, um die Anzahl der Wurzeln von (1) zu ermitteln, nur zu sehen, wie viele Wurzeln (1) und (2) gemeinschaftlich sind. Wir bestimmen also den grössten gemeinschaftlichen Divisor der Polynome $f(x)$ und $x^{p-1} - 1$; der Grad dieses Divisors giebt an, wie viele Wurzeln die Congruenz (1) besitzt.

Beispiel. Um die Anzahl der Wurzeln der Congruenz

(1) $$3x^3 - 5x^2 - x + 4 \equiv 0 \pmod{7}$$

zu bestimmen, haben wir den grössten gemeinschaftlichen Divisor von $x^6 - 1$ und $3x^3 - 5x^2 - x + 4$ zu suchen. Damit der Quotient der zu diesem Zwecke erforderlichen Division ganze Coefficienten erhalte, wollen wir den Coefficienten von x^3 in (1) auf die Einheit reduciren.

Da

$$-5 \equiv 9, \quad -1 \equiv 6, \quad 4 \equiv -3 \pmod{7}$$

ist, so geht (1) in

$$3x^3 + 9x^2 + 6x - 3 \equiv 0 \pmod{7}$$

oder in

(2) $$x^3 + 3x^2 + 2x - 1 \equiv 0 \pmod{7}$$

über. Dividiren wir jetzt $x^6 - 1$ durch $x^3 + 3x^2 + 2x - 1$, so bleibt der Rest

$$25x^2 + 35x - 15 \equiv 4x^2 - 1 \pmod{7}.$$

Ehe wir weiter dividiren, reduciren wir den Coefficienten von x^2 auf 1, indem wir beachten, dass

$$-1 \equiv -8 \pmod{7}$$

ist. Dann geht der Rest $4x^2 - 1$ in

$$4x^2 - 8 \equiv 4(x^2 - 2) \pmod{7}$$

über.

Mit $x^2 - 2$ dividiren wir weiter in $x^3 + 3x^2 + 2x - 1$ und erhalten als Rest

$$4x + 5 \equiv 4x + 12 \equiv 4(x + 3) \pmod{7}.$$

Wird jetzt endlich mit $x + 3$ in $x^2 - 2$ dividirt, so bleibt der Rest $7 \equiv 0 \pmod{7}$. Die Congruenz (1) hat daher mit $x^6 - 1 \equiv 0 \pmod{7}$ nur die eine Wurzel der Congruenz

$$x + 3 \equiv 0 \pmod{7},$$

d. i. 4 gemein, mit andern Worten: die Congruenz (1) besitzt überhaupt nur die eine Wurzel $x \equiv 4 \pmod{7}$.

Anmerkung. Der Lehrsatz I dieses Paragraphen liefert einen neuen Beweis des Wilson'schen Satzes. Die Congruenz

$$(x - 1)(x - 2) \ldots (x - \overline{p - 1}) - (x^{p-1} - 1) \equiv 0 \pmod{p}$$

ist offenbar vom Grade $p - 2$ und hat dabei die $p - 1$ Wurzeln 1, 2, 3, ..., $(p - 1)$. Sie muss daher eine identische Congruenz, d. h. jeder ihrer Coefficienten muss durch p theilbar sein; also ist auch der Coefficient des von x unabhängigen Gliedes durch p theilbar, oder

$$1 \cdot 2 \cdot 3 \ldots (p - 1) + 1 \equiv 0 \pmod{p}.$$

Viertes Kapitel.

Kettenbrüche.

§ 33. Definition. — Unter einem Kettenbruch versteht man einen Bruch, dessen Zähler eine ganze Zahl und dessen Nenner die Summe aus einer ganzen Zahl und einem Bruche von derselben Beschaffenheit sind. Ein Kettenbruch ist daher jeder Ausdruck von der Form

$$\alpha + \cfrac{b}{\beta + \cfrac{c}{\gamma + \cfrac{d}{\delta + \text{u. s. w.};}}}$$

darin bezeichnen $\alpha, \beta, \gamma, \delta, \ldots$, sowie $b, c, d, \ldots$ positive oder negative ganze Zahlen. Wir werden aber nur solche Kettenbrüche betrachten, in denen die Zähler $b, c, d, \ldots$ der Einheit gleich sind, welche also die Form

$$\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\delta + \cdot}}}$$

haben, wo übrigens $\alpha, \beta, \gamma, \delta, \ldots$ irgendwelche positive oder negative ganze Zahlen sind; denn diese Kettenbrüche sind die einzigen, die wir später anzuwenden haben.

„Die Kettenbrüche bieten sich uns naturgemäss jedesmal dar, wo es sich darum handelt, gebrochene oder irrationale Grössen in Zahlen auszudrücken. Nehmen wir nämlich an, wir hätten den Werth einer beliebigen gegebenen Grösse x anzugeben, die nicht durch eine ganze Zahl ausgedrückt werden kann, so wird der einfachste Weg darin bestehen, dass wir zunächst diejenige ganze Zahl aufsuchen, welche dem Werthe von x am nächsten liegt und sich von demselben nur durch einen Bruch unterscheidet, der kleiner als die Einheit ist. Diese ganze Zahl sei α, so ist $x - \alpha$ gleich einem

Bruche, der kleiner als 1 ist, folglich $\frac{1}{x-a}$ eine Zahl, welche grösser als 1 ist. Es sei daher $\frac{1}{x-a} = x_1$, und da x_1 grösser als die Einheit ist, so kann man die ganze Zahl bestimmen, welche dem Werthe von x_1 am nächsten liegt. Wird diese ganze Zahl a_1 genannt, so ist wieder $x_1 - a_1$ gleich einem Bruche, der kleiner als die Einheit ist, folglich $\frac{1}{x_1 - a_1}$ eine Zahl, die grösser als 1 ist, und die man mit x_2 bezeichnen kann. Um den Werth von x_2 zu ermitteln, hat man nur die demselben zunächst liegende ganze Zahl zu ermitteln; wird diese mit a_2 bezeichnet, so ist $x_2 - a_2$ kleiner als 1, folglich $\frac{1}{x_2 - a_2}$ gleich einer Grösse x_3, welche grösser als die Einheit ist, u. s. f. Durch dieses Verfahren muss man offenbar nach und nach dem Werthe von x immer näher kommen und zwar auf die einfachste und schnellste Weise, die möglich ist, da man nur ganze Zahlen anwendet, von denen jede dem gesuchten Werthe so nahe wie möglich liegt.

„Da jetzt

$$\frac{1}{x-a} = x_1$$

ist, so hat man

$$x - a = \frac{1}{x_1}, \quad \text{also} \quad x = a + \frac{1}{x_1};$$

ebenso folgt aus

$$\frac{1}{x_1 - a_1} = x_2, \quad \text{dass} \quad x_1 = a_1 + \frac{1}{x_2},$$

und aus

$$\frac{1}{x_2 - a_2} = x_3, \quad \text{dass} \quad x_2 = a_2 + \frac{1}{x_3}$$

ist, u. s. w., so dass man durch Einsetzung dieser Werthe der Reihe nach

$$x = a + \frac{1}{x_1}$$

$$= a + \frac{1}{a_1 + \frac{1}{x_2}}$$

$$= a + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{x_3}}}$$

und allgemein

$$x = a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

erhält.

„Es ist gut zu beachten, dass jede der ganzen Zahlen a, a_1, a_2, a_3, ..., welche, wie wir soeben gesehen haben, die den Grössen x, x_1, x_2, ... zunächst liegenden ganzzahligen Werthe darstellen, auf zwei verschiedene Arten genommen werden kann, da jede gegebene reelle Grösse, die nicht selbst eine ganze Zahl ist, zwischen zwei auf einander folgenden ganzen Zahlen liegt, von denen jede als angenäherter Werth gewählt werden kann. Hinsichtlich des Kettenbruchs, zu dem wir gelangen, besteht aber zwischen den beiden Arten, diese angenäherten Werthe zu wählen, ein wesentlicher Unterschied. Nimmt man nämlich immer diejenigen ganzen Zahlen, welche kleiner sind als die auszuwerthenden Grössen, so werden die Nenner a_1, a_2, a_3 ... sämmtlich positiv sein; dieselben werden sämmtlich negativ sein, wenn man immer die ganzen Zahlen nimmt, welche grösser als die auszuwerthenden Grössen sind, und sie werden zum Theil positiv, zum Theil negativ sein, wenn man bald zu kleine, bald zu grosse angenäherte Werthe wählt." (Lagrange, Zusätze zu Eulers Algebra).

Wir setzen für die Folge voraus, dass immer die unterhalb der zu bestimmenden Grössen liegenden ganzen Zahlen als angenäherte Werthe genommen, dass also die Zahlen a, a_1, a_2, ... sämmtlich positiv seien.

Wenn eine der Grössen x_1, x_2, x_3, ... eine ganze Zahl ist, so ist der Kettenbruch beendet. Ist z. B. x_2 eine ganze Zahl, so erhält man für x den Kettenbruch

$$a + \cfrac{1}{a_1 + \cfrac{1}{x_2}}.$$

Dieser Fall wird immer eintreten, wenn x durch einen rationalen Bruch ausgedrückt ist; wenn aber x eine irrationale oder eine transcendente Grösse ist, so wird der Kettenbruch ins Unendliche fortgehen.

§ 34. Verwandlung eines rationalen Bruchs in einen Kettenbruch. — Es sei $\frac{A}{B}$ ein rationaler Bruch, des-

sen Zähler und Nenner prim zu einander seien; dann ist die ganze Zahl a, die dem Werthe von $\frac{A}{B}$ am nächsten liegt, der Quotient der Division von A durch B. Wird der Rest dieser Division C genannt, so ist $\frac{A}{B} - a = \frac{C}{B}$. Es ist also $x_1 = \frac{B}{C}$, und um die ganze Zahl a_1 zu erhalten, die dem Werthe von $\frac{B}{C}$ am nächsten liegt, haben wir nur B durch C zu dividiren und den Quotienten dieser Division a_1 zu nennen. Wird der Rest dieser Division D genannt, so ist $x_1 - a_1 = \frac{D}{C}$, folglich $x_2 = \frac{C}{D}$; wir werden also weiter C durch D dividiren, den Quotienten a_2 nennen, u. s. f.

Um also einen gemeinen Bruch in einen Kettenbruch zu verwandeln, dividiren wir den Zähler desselben durch seinen Nenner und nennen den Quotienten a; darauf dividiren wir den Nenner durch den Rest und nennen den Quotienten a_1; hierauf dividiren wir den ersten Rest durch den zweiten und nennen den Quotienten a_2; in dieser Weise fahren wir fort, d. h. wir dividiren immer den vorletzten Rest durch den letzten, bis wir zu einer Division gelangen, welche den Rest Null liefert, was nothwendig einmal geschehen wird, da die Reste eine Reihe abnehmender positiver Zahlen bilden. Der aus den erhaltenen Quotienten $a, a_1, a_2, \ldots$ gebildete Kettenbruch

$$a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}},$$

für den wir zuweilen auch $(a, a_1, a_2, \ldots)$ schreiben werden, ist dann gleich dem gegebenen Bruch $\frac{A}{B}$.

Beispiele.

$$\text{I.}\quad \frac{379}{161} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3}}}}}} = (2, 2, 1, 4, 1, 2, 3)$$

$$\text{II.}\quad \frac{241}{1760} = \cfrac{1}{7 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{7}}}}} = (0, 7, 3, 3, 3, 7)$$

III. $\frac{1707}{505} = (3, 2, 1, 1, 1, 2, 2, 1, 1, 1, 2)$.

IV. $\frac{225}{157} = (1, 2, 3, 4, 5)$.

Das hier dargelegte Verfahren dient auch dazu, irgend eine durch einen Decimalbruch ausgedrückte Grösse in einen Kettenbruch zu verwandeln.

Beispiel.

V. $0{,}371317 = (0, 2, 1, 2, 3, 1, 6, 1, 1, 5, 32, 11)$.

§ 35. Bildung der Näherungsbrüche. — Bricht man einen Kettenbruch

$$a + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

bei irgend einer der ganzen Zahlen $a, a_1, a_2, \ldots$, die man im Gegensatz zu den vollständigen Quotienten $x_1, x_2, \ldots$ die unvollständigen Quotienten nennt, ab, so erhält man einen Näherungsbruch. So ist a der erste,

$$a + \frac{1}{a_1} = \frac{aa_1 + 1}{a_1}$$

der zweite,

$$a + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{aa_1 a_2 + a_2 + a}{a_1 a_2 + 1}$$

der dritte Näherungsbruch, u. s. w.

Um das Bildungsgesetz der Näherungsbrüche zu ermitteln, wollen wir den ersten mit $\frac{Z_1}{N_1}$, den zweiten mit $\frac{Z_2}{N_2}$, allgemein den k^{ten} mit $\frac{Z_k}{N_k}$ bezeichnen. Es ist dann $\frac{Z_1}{N_1} = \frac{a}{1}$,

$$\frac{Z_2}{N_2} = \frac{aa_1 + 1}{a_1} = \frac{Z_1 a_1 + 1}{N_1 a_1},$$

$$\frac{Z_3}{N_3} = \frac{a_2(aa_1 + 1) + a}{a_2 a_1 + 1} = \frac{a_2 Z_2 + Z_1}{a_2 N_2 + N_1}.$$

Wir werden jetzt beweisen, dass allgemein

$$\left\{ \frac{Z_n}{N_n} = \frac{a_{n-1} Z_{n-1} + Z_{n-2}}{a_{n-1} N_{n-1} + N_{n-2}} \right.$$

ist, dass also der Zähler, resp. Nenner, des n^{ten} Näherungsbruchs gefunden wird, indem man den Zähler, resp. Nenner, des $(n-1)^{\text{ten}}$ Näherungsbruchs mit dem n^{ten} unvollständigen

Quotienten a_{n-1} multiplicirt und zum Produkte den Zähler, resp. Nenner, des $(n-2)^{\text{ten}}$ Näherungsbruchs addirt.

Da der Satz für den dritten Näherungsbruch richtig ist, so haben wir, um seine allgemeine Gültigkeit nachzuweisen, nur darzuthun, dass, wenn derselbe bis zu einer gewissen Grenze, etwa bis zum k^{ten} Näherungsbruche, Geltung hat, er auch über diese Grenze hinaus für den $(k+1)^{\text{ten}}$ Näherungsbruch besteht. Es sei also

$$\frac{Z_k}{N_k} = \frac{a_{k-1} Z_{k-1} + Z_{k-2}}{a_{k-1} N_{k-1} + N_{k-2}}.$$

Wir erhalten hieraus den folgenden Näherungsbruch, wenn wir a_{k-1} durch $a_{k-1} + \frac{1}{a_k}$ ersetzen. Dies liefert

$$\frac{Z_{k+1}}{N_{k+1}} = \frac{\left(a_{k-1} + \frac{1}{a_k}\right) Z_{k-1} + Z_{k-2}}{\left(a_{k-1} + \frac{1}{a_k}\right) N_{k-1} + N_{k-2}}$$

$$= \frac{(a_{k-1}\, a_k + 1)\, Z_{k-1} + a_k\, Z_{k-2}}{(a_{k-1}\, a_k + 1)\, N_{k-1} + a_k\, N_{k-2}}$$

$$= \frac{a_k\, (a_{k-1}\, Z_{k-1} + Z_{k-2}) + Z_{k-1}}{a_k\, (a_{k-1}\, N_{k-1} + N_{k-2}) + N_{k-1}},$$

oder, wenn $a_{k-1} Z_{k-1} + Z_{k-2}$ durch Z_k und ebenso

$$a_{k-1}\; N_{k-1} + N_{k-2}$$

durch N_k ersetzt wird,

$$\frac{Z_{k+1}}{N_{k+1}} = \frac{a_k\, Z_k + Z_{k-1}}{a_k\, N_k + N_{k-1}},$$

und damit ist der Satz bewiesen.

Wenn wir den fingirten Näherungsbruch $\frac{Z_0}{N_0} = \frac{1}{0}$ als ersten vorausschicken, so liefert die hergeleitete Formel auch noch den zweiten Näherungsbruch, da sich dann

$$\frac{Z_2}{N_2} = \frac{a_1\, Z_1 + Z_0}{a_1\, N_1 + N_0} = \frac{a_1\, a + 1}{a_1 \cdot 1 + 0} = \frac{a_1\, a + 1}{a_1}$$

ergiebt. Dies soll in Zukunft geschehen, es soll also $\frac{Z_n}{N_n}$ den $(n+1)^{\text{ten}}$ Näherungsbruch bezeichnen.

Die Näherungsbrüche eines Kettenbruchs werden also in folgender Weise berechnet:

Man schreibt die unvollständigen Quotienten neben einander und setzt unter den ersten den Näherungsbruch $\frac{1}{0}$, unter den zweiten $\frac{a}{1}$. Darauf bildet man der Reihe nach die Zähler und Nenner der folgenden Näherungsbrüche, indem man jeden unvollständigen Quotienten mit dem Zähler, resp. Nenner, des unter ihm stehenden Näherungsbruches multiplicirt und zum Produkte den Zähler, resp. Nenner des diesem vorangehenden Näherungsbruches addirt.

Danach haben die oben in § 34 in Kettenbrüche verwandelten Brüche folgende Näherungsbrüche:

I.

2	2	1	4	1	2	3	
1	2	5	7	33	40	113	379
0	1	2	3	14	17	48	161

II.

0	7	3	3	3	7	
1	0	1	3	10	33	241
0	1	7	22	73	241	1760

III.

3	2	1	1	1	2	2	1	1	1	2	
1	3	7	10	17	27	71	169	240	409	649	1707
0	1	2	3	5	8	21	50	71	121	192	505

IV.

1	2	3	4	5	
1	1	3	10	43	225
0	1	2	7	30	157

V.

0	2	1	2	3	1	6	1	. .
1	0	1	1	3	10	13	88	. . .
0	1	2	3	8	27	35	237	

Anmerkung. Der erste unvollständige Quotient a kann auch Null sein; in diesem Falle darf man aber nicht vergessen, ihn hinzu schreiben und darunter den (zweiten) Näherungsbruch $\frac{0}{1}$ zu setzen.

§ 36. Eigenschaften der Näherungsbrüche.

Lehrsatz I. Bezeichnet $\frac{Z_n}{N_n}$ den $(n+1)^{\text{ten}}$ Näherungsbruch, so ist

$$(-1)^n (Z_n N_{n-1} - Z_{n-1} N_n) = +1 .$$

Beweis. Wir betrachten die Differenz zweier auf einander folgenden Näherungsbrüche $\frac{Z_n}{N_n}$ und $\frac{Z_{n-1}}{N_{n-1}}$. Es ergiebt sich

$$\frac{Z_n}{N_n} - \frac{Z_{n-1}}{N_{n-1}} = \frac{a_{n-1} Z_{n-1} + Z_{n-2}}{a_{n-1} N_{n-1} + N_{n-2}} - \frac{Z_{n-1}}{N_{n-1}}$$
$$= \frac{-(Z_{n-1} N_{n-2} - Z_{n-2} N_{n-1})}{N_n N_{n-1}};$$

es ist also

$$Z_n N_{n-1} - Z_{n-1} N_n = -(Z_{n-1} N_{n-2} - Z_{n-2} N_{n-1}) .$$

Daraus geht hervor, dass die Grösse

$$P = (-1)^n \{Z_n N_{n-1} - Z_{n-1} N_n\}$$

für jedes n denselben Werth hat. Da nun

$$Z_1 = a, \quad N_1 = 1, \quad Z_0 = 1, \quad N_0 = 0,$$

also für $n = 1$

$$P = (-1)^1 . (-1) = +1$$

ist, so ist für jeden Werth von n

$$(-1)^n (Z_n N_{n-1} - Z_{n-1} N_n) = +1 .$$

Aus diesem Satze geht unmittelbar hervor, dass Zähler und Nenner eines Näherungsbruches relative Primzahlen sind; denn ein etwa vorhandener gemeinschaftlicher Divisor von Z_n und N_n müsste auch in 1 aufgehen.

Ferner lehrt der Satz, dass die Differenz zweier auf einander folgenden Näherungsbrüche ein Bruch ist, welcher zum Zähler die Einheit und zum Nenner das Produkt der Nenner der Näherungsbrüche hat; denn es ist

$$\frac{Z_n}{N_n} - \frac{Z_{n-1}}{N_{n-1}} = \frac{(-1)^n}{N_n N_{n-1}} .$$

Lehrsatz II. Der Werth einer in einen Kettenbruch entwickelten Grösse liegt zwischen zwei aufeinander folgenden Näherungsbrüchen und zwar näher dem folgenden als dem vorhergehenden.

Beweis.

Ist $x = a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{x_n}}}}$,

so geht der $(n+1)^{\text{te}}$ Näherungsbruch

$$\frac{Z_n}{N_n} = \frac{a_{n-1} Z_{n-1} + Z_{n-2}}{a_{n-1} N_{n-1} + N_{n-2}}$$

offenbar in x über, wenn man a_{n-1} durch $a_{n-1} + \frac{1}{x_n}$ ersetzt. Es ist also

$$x = \frac{\left(a_{n-1} + \frac{1}{x_n}\right) Z_{n-1} + Z_{n-2}}{\left(a_{n-1} + \frac{1}{x_n}\right) N_{n-1} + N_{n-2}}$$

$$= \frac{x_n (a_{n-1} Z_{n-1} + Z_{n-2}) + Z_{n-1}}{x_n (a_{n-1} N_{n-1} + N_{n-2}) + N_{n-1}}$$

$$= \frac{x_n Z_n + Z_{n-1}}{x_n N_n + N_{n-1}}$$

und

$$x - \frac{Z_n}{N_n} = \frac{x_n Z_n + Z_{n-1}}{x_n N_n + N_{n-1}} - \frac{Z_n}{N_n} = \frac{Z_{n-1} N_n - Z_n N_{n-1}}{N_n (x_n N_n + N_{n-1})},$$

somit nach Lehrsatz I

$$(1) \qquad x - \frac{Z_n}{N_n} = \frac{-(-1)^n}{N_n (x_n N_n + N_{n-1})}.$$

Ebenso ergiebt sich

$$x - \frac{Z_{n-1}}{N_{n-1}} = \frac{x_n (Z_n N_{n-1} - Z_{n-1} N_n)}{N_{n-1} (x_n N_n + N_{n-1})}$$

oder

$$(2) \qquad x - \frac{Z_{n-1}}{N_{n-1}} = \frac{(-1)^n x_n}{N_{n-1} (x_n N_n + N_{n-1})}.$$

Da x_n positiv ist, so haben die rechten Seiten der Gleichungen (1) und (2) entgegengesetzte Vorzeichen, also liegt x zwischen $\frac{Z_{n-1}}{N_{n-1}}$ und $\frac{Z_n}{N_n}$. Da ausserdem $x_n > 1$ und $N_{n-1} < N_n$ ist, so ist die Differenz (2) grösser als die Differenz (1), d. h. x liegt näher an $\frac{Z_n}{N_n}$ als an $\frac{Z_{n-1}}{N_{n-1}}$.

Der erste Näherungsbruch ist $\frac{1}{0} = \infty$, der zweite a; letzterer ist $< x$, folglich ist nach dem eben bewiesenen Satze der dritte $> x$, mithin der vierte wieder $< x$, u. s. w. Es sind also die Näherungsbrüche gerader Ordnung sämmtlich $< x$, und da jeder folgende näher an x liegt, als der vorhergehende, so bilden dieselben eine steigende Reihe. Dagegen sind die Näherungsbrüche ungerader Ordnung sämmtlich $> x$, und da jeder folgende näher an x liegt, als der vorhergehende, so bilden dieselbe eine fallende Reihe.

Zusatz I. Die Differenz zwischen einer in einen Kettenbruch entwickelten Grösse und dem n^{ten} Näherungsbruch desselben ist, abgesehen vom Vorzeichen, kleiner als $\frac{1}{N_{n-1} N_n}$ und grösser als $\frac{1}{N_{n-1}(N_n + N_{n-1})}$.

Beweis. Die Gleichung (2) lässt sich auch in folgender Weise schreiben:

$$x - \frac{Z_{n-1}}{N_{n-1}} = \frac{(-1)^n}{N_{n-1}\left(N_n + \frac{N_{n-1}}{x_n}\right)},$$

und da x_n zwischen 1 und ∞ enthalten ist, so liegt die betrachtete Differenz zwischen

$$\frac{(-1)^n}{N_{n-1}(N_n + N_{n-1})} \text{ und } \frac{(-1)^n}{N_{n-1} N_n}.$$

Zuzatz II. Die Differenz zwischen dem Werth eines Kettenbruchs und dem n^{ten} Näherungsbruch ist kleiner als die Einheit, dividirt durch das Quadrat des Nenners des Näherungsbruchs.

Beweis. Da $x - \frac{Z_{n-1}}{N_{n-1}} < \frac{(-1)^n}{N_{n-1} N_n}$ und $N_{n-1} < N_n$ ist, so ist um so mehr

$$x - \frac{Z_{n-1}}{N_{n-1}} < \frac{(-1)^n}{N_{n-1}^2}.$$

Zusatz III. Wenn die in einen Kettenbruch entwickelte Grösse x irrational ist, so lässt sich immer ein Näherungsbruch von der Beschaffenheit bilden, dass die Differenz zwischen demselben und x kleiner als eine beliebig gegebene Grösse α sei.

Beweis. Da $x - \frac{Z_{n-1}}{N_{n-1}} < \frac{(-1)^n}{N_{n-1}^2}$ ist, so wird diese Differenz gewiss $< \alpha$ sein, wenn $\frac{1}{N_{n-1}^2} < \alpha$, also $N_{n-1}^2 > \frac{1}{\alpha}$, d. h. $N_{n-1} > \sqrt{\frac{1}{\alpha}}$ ist, und da die Nenner der auf einander folgenden Näherungsbrüche eine Reihe zunehmender Zahlen bilden, so lässt sich immer ein N ermitteln, welches dieser Bedingung genügt.

Lehrsatz III. Wenn ein irreducibeler Bruch $\frac{A}{B}$ zwischen zwei auf einander folgenden Näherungsbrüchen $\frac{Z_{n-1}}{N_{n-1}}$ und $\frac{Z_n}{N_n}$ liegt, so ist sein Nenner grösser als der Nenner jedes der beiden Näherungsbrüche.

Beweis. Da $\frac{A}{B}$ zwischen $\frac{Z_{n-1}}{N_{n-1}}$ und $\frac{Z_n}{N_n}$ liegt, so ist

$$\frac{Z_{n-1}}{N_{n-1}} \gtrless \frac{A}{B} \gtrless \frac{Z_n}{N_n},$$

je nachdem $\frac{Z_{n-1}}{N_{n-1}} \gtrless \frac{Z_n}{N_n}$ ist. In jedem Falle haben die beiden Differenzen

$$\frac{A}{B} - \frac{Z_{n-1}}{N_{n-1}} \text{ und } \frac{Z_n}{N_n} - \frac{Z_{n-1}}{N_{n-1}}$$

dasselbe Vorzeichen, und der absolute Werth der letzten Differenz, d. i. $\frac{1}{N_n N_{n-1}}$, ist grösser als der absolute Werth der ersteren. Es ist also, wenn wir den absoluten Werth einer Zahl dadurch ausdrücken, dass wir dieselbe in eine eckige Klammer [ ] setzen,

$$\left[\frac{A}{B} - \frac{Z_{n-1}}{N_{n-1}}\right] < \left[\frac{1}{N_n N_{n-1}}\right],$$

und daraus folgt leicht

$$[A N_{n-1} - B Z_{n-1}] < \frac{B}{N_n}.$$

Die linke Seite ist eine ganze Zahl und der Voraussetzung nach von Null verschieden; folglich muss $B > N_n$ und um so mehr $B > N_{n-1}$ sein.

§ 37. Symmetrische Kettenbrüche. — Wenn a, a_1, $a_2, \ldots, a_{n-1}$ die unvollständigen Quotienten eines Kettenbruches sind, und man

$$a = a_{n-1}, \; a_1 = a_{n-2}, \text{ u. s. w.}$$

hat, wenn also die von den Enden gleich weit entfernten unvollständigen Quotienten einander gleich sind, so nennt man den Kettenbruch symmetrisch. Von dieser Art sind z. B. die Entwicklungen der Brüche

$$\frac{450}{199} \text{ (unvollst. Quotienten: 2, 3, 1, 4, 1, 3, 2)},$$

$$\frac{28013}{5156} \text{ (unvollst. Quotienten: 5, 2, 3, 4, 4, 3, 2, 5)}.$$

Lehrsatz I. Wenn ein rationaler Bruch $\frac{Z}{N}$, der grösser als die Einheit ist, einen symmetrischen Kettenbruch liefert, so ist entweder $N^2 + 1$ oder $N^2 - 1$ durch Z theilbar.

Beweis. Wir nehmen an, es sei

$$(1) \qquad \frac{Z}{N} = a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1}}}}.$$

Wird der vorletzte Näherungsbruch (der letzte ist $\frac{Z}{N}$ selbst) mit $\frac{Z_{n-1}}{N_{n-1}}$ bezeichnet, so ist nach dem Früheren

$$Z \quad = a_{n-1} Z_{n-1} + Z_{n-2}, \text{ also } \frac{Z}{Z_{n-1}} = a_{n-1} + \frac{Z_{n-2}}{Z_{n-1}}$$

$$Z_{n-1} = a_{n-2} Z_{n-2} + Z_{n-3}, \text{ also } \frac{Z_{n-1}}{Z_{n-2}} = a_{n-2} + \frac{Z_{n-3}}{Z_{n-2}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Z_3 = a_2 Z_2 + Z_1, \text{ also } \frac{Z_3}{Z_2} = a_2 + \frac{Z_1}{Z_2}$$

$$Z_2 = a_1 Z_1 + Z_0, \text{ also } \frac{Z_2}{Z_1} = a_1 + \frac{Z_0}{Z_1}$$

$$\frac{Z_0}{Z_1} = \frac{1}{a}.$$

Daraus geht hervor, dass der Kettenbruch

$$(2) \qquad a_{n-1} + \cfrac{1}{a_{n-2} + \cdots + \cfrac{1}{a_1 + \cfrac{1}{a}}},$$

welcher dieselben unvollständigen Quotienten wie (1), aber in umgekehrter Reihenfolge enthält, die Entwicklung von $\frac{Z}{Z_{n-1}}$ ist. Wenn nun (1) ein symmetrischer Kettenbruch ist, so ist er mit (2) identisch; in diesem Falle hat man also

$$\frac{Z}{N} = \frac{Z}{Z_{n-1}}$$

oder

$$N = Z_{n-1},$$

d. h. der Nenner des Bruchs ist gleich dem Zähler des vorletzten Näherungsbruchs. Wird dieser Werth von Z_{n-1} in die Formel

$$ZN_{n-1} - NZ_{n-1} = (-1)^n$$

eingesetzt, so geht dieselbe über in

$$ZN_{n-1} - N^2 = (-1)^n,$$

und hieraus folgt, dass

$$\frac{N^2 \pm 1}{Z} = N_{n-1},$$

also eine ganze Zahl ist.

Lehrsatz II. (Umkehrung). Wenn $N^2 \pm 1$ durch Z theilbar ist, so wird der Kettenbruch, den die Entwicklung von $\frac{Z}{N}$ liefert, symmetrisch sein.

Beweis. Man kann bei der Entwicklung eines rationalen Bruchs in einen Kettenbruch es stets so einrichten, dass die Anzahl der unvollständigen Quotienten nach Belieben gerade oder ungerade sei; denn wenn a_{n-1} der letzte unvollständige Quotient, also > 1 ist, so kann man dafür immer $(a_{n-1} - 1) + \frac{1}{1}$ schreiben, wodurch die Anzahl n der unvollständigen Quotienten um eine Einheit vergrössert wird.

Dies vorausgesetzt, entwickeln wir $\frac{Z}{N}$ so in einen Kettenbruch, dass die Anzahl n der unvollständigen Quotienten gerade oder ungerade sei, je nachdem $N^2 + 1$ oder $N^2 - 1$ durch Z theilbar sein soll. Es ist dann $\frac{N^2 + (-1)^n}{Z} = R$ eine ganze Zahl, also

(1) $$RZ - N^2 = (-1)^n.$$

Da nun $\frac{Z_{n-1}}{N_{n-1}}$ der vorletzte Näherungsbruch ist, so haben wir ausserdem

$$(2)\qquad ZN_{n-1} - Z_{n-1}N = (-1)^n\,,$$

und aus diesen beiden Gleichungen folgt

$$Z(R - N_{n-1}) = N(N - Z_{n-1})\,.$$

Die rechte Seite dieser Gleichung muss also durch Z theilbar sein. Nun ist Z prim zu N; Z muss demnach in $N - Z_{n-1}$ aufgehen, und da diese Differenz $< Z$ ist, so muss sie Null, d. h.

$$N = Z_{n-1}$$

sein. Dann ist aber der Kettenbruch, den die Entwicklung von $\frac{Z}{N}$ liefert, identisch mit demjenigen, welchen man durch Entwicklung von $\frac{Z}{Z_{n-1}}$ erhält, d. h. er ist symmetrisch.

Lehrsatz III. *Wenn eine ganze Zahl P ohne Rest in die Summe zweier Quadrate aufgeht, welche prim zu einander sind, so ist sie selbst die Summe zweier Quadrate.*

Beweis. Es seien R und S relative Primzahlen, und es möge P in $R^2 + S^2$ aufgehen. Wird dann $\frac{R}{S}$ in einen Kettenbruch entwickelt und der vorletzte Näherungsbruch mit $\frac{r}{s}$ bezeichnet, so ist

$$Rs - Sr = \pm 1\,.$$

Da nun die Zahl P in $R^2 + S^2$ aufgeht, so geht dieselbe auch in

$$\begin{aligned}(R^2 + S^2)(r^2 + s^2) &= (Rr + Ss)^2 + (Rs - Sr)^2 \\ &= (Rr + Ss)^2 + 1\,,\end{aligned}$$

also auch für jeden Werth der ganzen Zahl k in

$$(Rr + Ss - kP)^2 + 1$$

auf.

Ueber die unbestimmte Grösse k kann man so verfügen, dass die Zahl

$$Q = Rr + Ss - kP < P$$

werde. Wir können also unter der gemachten Voraussetzung eine ganze Zahl $Q < P$ so bestimmen, dass

$$\frac{Q^2 + 1}{P}$$

eine ganze Zahl ist.

Wenn wir also $\frac{P}{Q}$ in einen Kettenbruch entwickeln und es dabei so einrichten, dass die Anzahl der unvollständigen Quotienten gerade sei, so wird dieser Kettenbruch symmetrisch werden, und die Reihe der unvollständigen Quotienten wird sich folgendermassen schreiben lassen:

$$a,\ a_1,\ a_2,\ \ldots,\ a_{m-1},\ a_{m-1},\ \ldots,\ a_2,\ a_1,\ a.$$

Der aus der ersten Hälfte dieser Zahlen gebildete Kettenbruch ist $\frac{Z_m}{N_m}$, der aus der letzten Hälfte gebildete der vollständige Quotient x_m. Da dieser letztere aber dieselben unvollständigen Quotienten wie der erste, nur in umgekehrter Reihenfolge enthält, so ist er gleich $\frac{Z_m}{Z_{m-1}}$, und durch Einsetzung dieses Werthes für x_m in die Gleichung

$$\frac{P}{Q} = \frac{Z_m x_m + Z_{m-1}}{N_m x_m + N_{m-1}}$$

erhält man

$$\frac{P}{Q} = \frac{Z_m^2 + Z_{m-1}^2}{Z_m N_m + Z_{m-1} N_{m-1}}.$$

Die rechte Seite dieser Formel ist ebenso wie die linke ein irreducibeler Bruch. Es ist nämlich

$$Z_m (Z_m N_m + Z_{m-1} N_{m-1}) - N_m (Z_m^2 + Z_{m-1}^2)$$
$$= Z_{m-1} (Z_m N_{m-1} - Z_{m-1} N_m) = (-1)^m Z_{m-1}.$$

Eine Zahl, welche in den Zähler und Nenner der rechten Seite der obigen Formel aufginge, müsste also auch in Z_{m-1} und somit auch in Z_m aufgehen, während diese Zahlen prim zu einander sind. Es ist daher

$$P = Z_m^2 + Z_{m-1}^2,$$

und das sollte bewiesen werden.

Die letzte Formel lehrt nicht bloss, dass P in zwei Quadrate zerfällt werden kann, sondern bestimmt auch die Grösse dieser Quadrate, wie aus den folgenden Beispielen ersichtlich sein wird.

Beispiele. I. Die Zahl 97 geht ohne Rest in $22^2 + 1$ auf; sie geht also für jeden Werth von k in $(22 - 97k)^2 + 1$ auf; am einfachsten ist es, $k = 0$ zu nehmen. Nun ist

$$\frac{97}{22} = 4 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{4}}},$$

und da die Berechnung der drei ersten Näherungsbrüche

4	2	
$\frac{1}{0}$	$\frac{4}{1}$	$\frac{9}{2}$

ergiebt, so ist $97 = 9^2 + 4^2$.

II. 757 geht ohne Rest in $87^2 + 1$ auf. Unvollständige Quotienten des Bruchs $\frac{757}{87}$:

$$8,\ 1,\ 2,\ 2,\ 1,\ 8.$$

Näherungsbrüche:

8	1	2	
$\frac{1}{0}$	$\frac{8}{1}$	$\frac{9}{1}$	$\frac{26}{3}$

Zerlegung: $757 = 26^2 + 9^2$.

III. 433 geht ohne Rest in $179^2 + 1$ auf. Unvollständige Quotienten des Bruchs $\frac{433}{179}$:

$$2,\ 2,\ 2,\ 1,\ 1,\ 2,\ 2,\ 2.$$

Näherungsbrüche:

2	2	2	1	
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{5}{2}$	$\frac{12}{5}$	$\frac{17}{7}$

Zerlegung: $433 = 17^2 + 12^2$.

IV. 977 geht ohne Rest in $252^2 + 1$ auf. Unvollständige Quotienten des Bruchs $\frac{977}{252}$:

$$3,\ 1,\ 7,\ 7,\ 1,\ 3.$$

Näherungsbrüche:

3	1	7	
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{31}{8}$

Zerlegung: $977 = 31^2 + 4^2$.

§ 38. Anwendung der Kettenbrüche zur Auf-

lösung der Congruenz ersten Grades mit einer Unbekannten. — Um die Congruenz

$$ax \equiv b \pmod{m},$$

d. i. die unbestimmte Gleichung

$$ax - my = b$$

aufzulösen, entwickeln wir $\frac{a}{m}$ in einen Kettenbruch und berechnen die Näherungsbrüche desselben. Der letzte dieser Näherungsbrüche ist $\frac{a}{m}$, der vorletzte werde mit $\frac{\alpha}{\mu}$ bezeichnet; dann ist nach dem Früheren

$$a\mu - \alpha m = \pm 1.$$

Dies vorausgesetzt, berechnen wir x und y mittels der gegebenen Gleichung

$$ax - my = b$$

und der Hülfsgleichung

$$\alpha x - \mu y = k,$$

in welcher k eine unbestimmte ganze Zahl bezeichnet. Es ergiebt sich

$$x = \frac{\mu b - m k}{a\mu - \alpha m} = \frac{\mu b - m k}{\pm 1},$$

$$y = \frac{\alpha b - a k}{a\mu - \alpha m} = \frac{\alpha b - a k}{\pm 1},$$

und somit ist die vorgelegte Gleichung in ganzen Zahlen aufgelöst.

Beispiele. I. $157x \equiv 72 \pmod{179}$.

$\frac{157}{179}$ liefert, in einen Kettenbruch entwickelt, die unvollständigen Quotienten

$$0,\ 1,\ 7,\ 7,\ 3.$$

Näherungsbrüche:

0	1	7	7	3	
1	0	1	7	50	157
0	1	1	8	57	179

Es sind also die Gleichungen

$$157x - 179y = 72$$

$$50x - 57y = k$$

aufzulösen; es ergiebt sich (auf y kommt es hier nicht an)

$$x = -4104 + 179k;$$

die Congruenz hat also die Wurzel

$$x \equiv -4104 \equiv 13 \pmod{179}.$$

II. $281x \equiv 400 \pmod{859}$.

Unvollständige Quotienten der Kettenbruch-Entwicklung von $\frac{281}{859}$:

$$0,\ 3,\ 17,\ 1,\ 1,\ 3,\ 2.$$

Näherungsbrüche:

0	3	17	1	1	3	2	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{3}$	$\frac{17}{52}$	$\frac{18}{55}$	$\frac{35}{107}$	$\frac{123}{376}$	$\frac{281}{859}$

Gleichungen:

$$281x - 859y = 400$$

$$123x - 376y = k.$$

Resultat:

$$x = -150400 + 859k,$$

d. i.

$$x \equiv 784 \pmod{859}.$$

Anmerkung. Wir haben im Vorstehenden die Lagrange'sche Methode in der von C. Reuschle jun. (Zeitschrift für Mathem. u. Physik, 1874, p. 272) vereinfachten Form gegeben.

§ 39. Irrationale Grössen, deren Entwicklungen in Kettenbrüche zu einem und demselben vollständigen Quotienten führen.

Lehrsatz I. Wenn die Kettenbrüche, in welche sich zwei irrationale Grössen x, x' entwickeln lassen, einen vollständigen Quotienten y gemeinsam haben, so besteht zwischen beiden eine Gleichung

$$x' = \frac{\alpha x + \beta}{\gamma x + \delta},$$

wo α, β, γ, δ ganze Zahlen sind, die der Bedingung

$$\alpha\delta - \beta\gamma = \pm 1$$

genügen.

Beweis. Wir denken uns x und x' in Kettenbrüche entwickelt; die Näherungsbrüche, welche in beiden dem vollständigen Quotienten y entsprechen, seien beziehungsweise $\frac{Z_k}{N_k}$, $\frac{Z'_m}{N'_m}$,

die vorhergehenden beziehungsweise $\frac{Z_{k-1}}{N_{k-1}}$, $\frac{Z'_{m-1}}{N'_{m-1}}$, so ist bekanntlich

$$x = \frac{Z_k y + Z_{k-1}}{N_k y + N_{k-1}}, \tag{1}$$

$$x' = \frac{Z'_m y + Z'_{m-1}}{N'_m y + N'_{m-1}}. \tag{2}$$

Aus (1) folgt

$$y = \frac{Z_{k-1} - N_{k-1} x}{N_k x - Z_k},$$

aus (2) ebenso

$$y = \frac{Z'_{m-1} - N'_{m-1} x'}{N'_m x' - Z'_m},$$

also ist

$$\frac{Z'_{m-1} - N'_{m-1} x'}{N'_m x' - Z'_m} = \frac{Z_{k-1} - N_{k-1} x}{N_k x - Z_k},$$

und diese Gleichung liefert, gehörig entwickelt,

$$x' = \frac{(Z'_m N_{k-1} - Z'_{m-1} N_k) x + (Z_k Z'_{m-1} - Z_{k-1} Z'_m)}{(N_{k-1} N'_m - N_k N'_{m-1}) x + (Z_k N'_{m-1} - Z_{k-1} N'_m)}$$

oder

$$x' = \frac{\alpha x + \beta}{\gamma x + \delta},$$

wo

$$\alpha = Z'_m N_{k-1} - Z'_{m-1} N_k,$$
$$\beta = Z_k Z'_{m-1} - Z_{k-1} Z'_m,$$
$$\gamma = N_{k-1} N'_m - N_k N'_{m-1},$$
$$\delta = Z_k N'_{m-1} - Z_{k-1} N'_m$$

und, wie die wirkliche Ausrechnung ergiebt,

$$\alpha\delta - \beta\gamma = (Z_k N_{k-1} - Z_{k-1} N_k)(Z'_m N'_{m-1} - Z'_{m-1} N'_m)$$
$$= (-1)^{k+m}$$

ist.

Lehrsatz II. (Umkehrung). Wenn zwischen zwei irrationalen Grössen x, x' die Gleichung

$$x' = \frac{\alpha x + \beta}{\gamma x + \delta} \tag{1}$$

besteht, wo α, β, γ, δ ganze Zahlen sind, die der Bedingung

$$\alpha\delta - \beta\gamma = \pm 1$$

genügen, so haben die Kettenbrüche, in welche sich x und x' entwickeln lassen, einen vollständigen Quotienten y gemeinschaftlich.

Beweis. Wir entwickeln x in einen Kettenbruch und nennen einen beliebig weit entfernten unvollständigen Quotienten y; demselben entspreche der Näherungsbruch $\frac{Z_k}{N_k}$, welchem $\frac{Z_{k-1}}{N_{k-1}}$ vorangehen möge. Dann ist

$$x = \frac{Z_k y + Z_{k-1}}{N_k y + N_{k-1}},$$

also

$$x' = \frac{(\alpha Z_k + \beta N_k) y + (\alpha Z_{k-1} + \beta N_{k-1})}{(\gamma Z_k + \delta N_k) y + (\gamma Z_{k-1} + \delta N_{k-1})}$$

oder kürzer

(2) $$x' = \frac{Ay + B}{Cy + D},$$

wo, wie sich leicht ergiebt,

(3) $$AD - BC = (\alpha\delta - \beta\gamma)(Z_k N_{k-1} - Z_{k-1} N_k) = \pm 1$$

ist. Nun ist

$$\frac{\alpha Z_k + \beta N_k}{\alpha Z_{k-1} + \beta N_{k-1}} = \frac{N_k}{N_{k-1}} \cdot \frac{\alpha \frac{Z_k}{N_k} + \beta}{\alpha \frac{Z_{k-1}}{N_{k-1}} + \beta};$$

der erste Factor der rechten Seite ist positiv und > 1; der zweite kann, da man $\frac{Z_k}{N_k}$ und $\frac{Z_{k-1}}{N_{k-1}}$ einander beliebig nähern kann, der Einheit so nahe gebracht werden, als man will; folglich ist die linke Seite positiv und grösser 1, d. h. $A > B$. Ebenso lässt sich zeigen, dass $C > D$ ist.

Entwickelt man jetzt den rationalen Bruch $\frac{A}{C}$ in einen Kettenbruch und bezeichnet den vorletzten Näherungsbruch desselben mit $\frac{B'}{D'}$, so ist

(4) $$AD' - CB' = \pm 1,$$

und es lässt sich, wie wir früher gesehen haben, stets so einrichten, dass in (4) das Zeichen $\pm$ dasselbe sei wie in (3). Dann folgt aus diesen beiden Gleichungen

$$A(D' - D) = C(B' - B).$$

Weil aber A prim zu C und $> B$, also um so mehr $> B'$ ist, so kann diese Gleichung nur bestehen, wenn $B = B'$, also $D = D'$ ist, und dann zeigt die Gleichung (2), dass y ein unvollständiger Quotient auch von x' ist.

§ 40. Verwandlung der irrationalen Wurzeln von Gleichungen zweiten Grades in Kettenbrüche. — Um die nachstehende allgemeine Darstellung verständlicher zu machen, wollen wir mit einem Beispiele beginnen.

Die Gleichung

$$3x^2 - 14x + 10 = 0$$

hat die Wurzeln $x = \frac{7 \pm \sqrt{19}}{3}$, von denen wir zunächst $\frac{7 + \sqrt{19}}{3}$ ins Auge fassen wollen. Die Wurzel der grössten Quadratzahl unter 19 ist 4, die grösste ganze Zahl, welche nicht grösser als $\frac{7 + \sqrt{19}}{3}$ ist, folglich 3; wir setzen demgemäss

$$\frac{7 + \sqrt{19}}{3} = 3 + \frac{7 + \sqrt{19} - 9}{3} = 3 + \frac{\sqrt{19} - 2}{3} = 3 + \frac{1}{x_1},$$

und es ist

$$x_1 = \frac{3}{\sqrt{19} - 2} = \frac{3(\sqrt{19} + 2)}{19 - 4} = \frac{\sqrt{19} + 2}{5}.$$

Da weiter 1 die grösste ganze Zahl ist, die nicht grösser als x_1 ist, so setzen wir

$$x_1 = 1 + \frac{\sqrt{19} + 2 - 5}{5} = 1 + \frac{\sqrt{19} - 3}{5} = 1 + \frac{1}{x_2}.$$

Ebenso ergiebt sich

$$x_2 = \frac{5}{\sqrt{19} - 3} = \frac{5(\sqrt{19} + 3)}{19 - 9} = \frac{\sqrt{19} + 3}{2} = 3 + \frac{\sqrt{19} + 3 - 6}{2}$$

$$= 3 + \frac{\sqrt{19} - 3}{2} = 3 + \frac{1}{x_3};$$

$$x_3 = \frac{2}{\sqrt{19} - 3} = \frac{2(\sqrt{19} + 3)}{19 - 9} = \frac{\sqrt{19} + 3}{5} = 1 + \frac{\sqrt{19} - 2}{5} = 1 + \frac{1}{x_4};$$

$$x_4 = \frac{5}{\sqrt{19} - 2} = \frac{5(\sqrt{19} + 2)}{19 - 4} = \frac{\sqrt{19} + 2}{3} = 2 + \frac{\sqrt{19} - 4}{3} = 2 + \frac{1}{x_5};$$

$$x_5 = \frac{3}{\sqrt{19}-4} = \frac{3(\sqrt{19}+4)}{19-16} = \frac{\sqrt{19}+4}{1} = 8 + \frac{\sqrt{19}-4}{1} = 8 + \frac{1}{x_6};$$

$$x_6 = \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{19-16} = \frac{\sqrt{19}+4}{3} = 2 + \frac{\sqrt{19}-2}{3}.$$

$\frac{\sqrt{19}-2}{3}$ ist aber wieder die Zahl, die wir oben mit $\frac{1}{x_1}$ bezeichnet haben; daher wiederholen sich von hier an die früheren Quotienten, sowohl die vollständigen, als auch die unvollständigen. Die Reihe der letzteren ist, wenn die sich wiederholenden in eine Klammer eingeschlossen werden,

$$3,\ (1,\ 3,\ 1,\ 2,\ 8,\ 2),\ (1,\ 3, \ldots), \ldots$$

Näherungsbrüche:

3	1	3	1	2	8	2	1	...	
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{15}{4}$	$\frac{19}{5}$	$\frac{53}{14}$	$\frac{443}{117}$	$\frac{939}{248}$	$\frac{1382}{365}$	$= 3,786301,$

was noch in der fünften Decimalstelle richtig ist.

Für die zweite Wurzel erhalten wir auf dieselbe Weise:

$$\frac{7-\sqrt{19}}{3} = \frac{1}{x_1};$$

$$x_1 = \frac{3(7+\sqrt{19})}{49-19} = \frac{7+\sqrt{19}}{10} = 1 + \frac{\sqrt{19}-3}{10} = 1 + \frac{1}{x_2},$$

$$x_2 = \frac{10(\sqrt{19}+3)}{19-9} = \frac{\sqrt{19}+3}{1} = 7 + \frac{\sqrt{19}-4}{1} = 7 + \frac{1}{x_3},$$

$$x_3 = \frac{\sqrt{19}+4}{19-16} = \frac{\sqrt{19}+4}{3} = 2 + \frac{\sqrt{19}-2}{3} = 2 + \frac{1}{x_4},$$

$$x_4 = \frac{3(\sqrt{19}+2)}{19-4} = \frac{\sqrt{19}+2}{5} = 1 + \frac{\sqrt{19}-3}{5} = 1 + \frac{1}{x_5},$$

$$x_5 = \frac{5(\sqrt{19}+3)}{19-9} = \frac{\sqrt{19}+3}{2} = 3 + \frac{\sqrt{19}-3}{2} = 3 + \frac{1}{x_6},$$

$$x_6 = \frac{2(\sqrt{19}+3)}{19-9} = \frac{\sqrt{19}+3}{5} = 1 + \frac{\sqrt{19}-2}{5} = 1 + \frac{1}{x_7},$$

$$x_7 = \frac{5(\sqrt{19}+2)}{19-4} = \frac{\sqrt{19}+2}{3} = 2 + \frac{\sqrt{19}-4}{3} = 2 + \frac{1}{x_8},$$

$$x_8 = \frac{3(\sqrt{19}+4)}{19-16} = \frac{\sqrt{19}+4}{1} = 8 + \frac{\sqrt{19}-4}{1} = 8 + \frac{1}{x_3}.$$

Die Reihe der unvollständigen Quotienten ist also

$$0,\ 1,\ 7,\ (2,\ 1,\ 3,\ 1,\ 2,\ 8),\ (2, \ldots), \ldots,$$

wo wieder die sich wiederholenden Quotienten in eine Klammer gesetzt sind.

Es sei jetzt allgemein

$$Ax^2 + 2Bx + C = 0$$

eine Gleichung zweiten Grades mit ganzen Coefficienten und $B^2 - AC = D$ positiv und keine Quadratzahl, so dass die Wurzeln der Gleichung, nämlich

$$x = \frac{-B \pm \sqrt{D}}{A}$$

oder, wenn für $\sqrt{D}$ der positive Werth genommen wird,

$$x = \frac{\mp B + \sqrt{D}}{\pm A}$$

irrational sind. Wir stellen uns die Aufgabe, eine der Wurzeln, etwa $\frac{-B + \sqrt{D}}{+A}$ in einen Kettenbruch zu entwickeln. Dabei setzen wir voraus, dass die Wurzel einen positiven Werth habe; sollte dies nicht der Fall sein, so würden wir $-x$ statt x in einen Kettenbruch entwickeln und vor die Entwicklung das Zeichen — setzen.

Bezeichnet nun r die Wurzel der grössten unter D liegenden Quadratzahl, so lässt sich die grösste ganze Zahl a bestimmen, die $< x$ ist (dieselbe kann auch Null sein). Wir setzen dann

$$x = a + \frac{-B + \sqrt{D} - aA}{A} = a + \frac{1}{x_1},$$

wo also

$$x_1 = \frac{A}{-(B + aA) + \sqrt{D}}$$

positiv und > 1 ist. Um den Nenner dieses Ausdrucks rational zu machen, multipliciren wir Zähler und Nenner mit $+(B + aA) + \sqrt{D}$ und erhalten

$$x_1 = \frac{A\,[(B + aA) + \sqrt{D}]}{D - (B + aA)^2}$$

oder, da $D = B^2 - AC$ ist,

$$x_1 = \frac{(B + aA) + \sqrt{D}}{-C - 2aB - a^2A} = \frac{B_1 + \sqrt{D}}{A_1},$$

und diese Grösse x_1 ist, wie wir gesehen haben, positiv und

grösser als 1. Somit ist die grösste in ihr enthaltene ganze Zahl, die wir a_1 nennen wollen, von Null verschieden, und wenn wir mit x_1 genau so verfahren, wie wir mit x verfuhren, so erhalten wir

$$x_1 = a_1 + \frac{1}{x_2};$$

darin ist x_2 eine positive Zahl > 1, welche die Form

$$x_2 = \frac{B_2 + \sqrt{D}}{A_2}$$

hat, und B_2, A_2 sind, ebenso wie B_1, A_1, ganze Zahlen. So fortfahrend erhalten wir für x die Entwicklung

$$x = a + \cfrac{1}{a_1 + \cfrac{}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{x_k}}}},$$

wo $x_k = \dfrac{B_k + \sqrt{D}}{A_k}$ ist, in welchem Ausdruck B_k und A_k ganze Zahlen sein werden.

Lehrsatz. Die Zahlen B_k und A_k, zu welchen die vorstehende Entwicklung führt, sind positiv für alle über eine gewisse Grenze hinausliegenden Werthe von k.

Beweis. Nach § 36 ist, wenn $\dfrac{Z_k}{N_k}$ den $(k+1)^{\text{ten}}$ und $\dfrac{Z_{k-1}}{N_{k-1}}$ den diesem vorhergehenden Näherungsbruch bezeichnet,

$$x = \frac{Z_k x_k + Z_{k-1}}{N_k x_k + N_{k-1}},$$

also

$$\frac{-B + \sqrt{D}}{A} = \frac{Z_k\left(\dfrac{B_k + \sqrt{D}}{A_k}\right) + Z_{k-1}}{N_k\left(\dfrac{B_k + \sqrt{D}}{A_k}\right) + N_{k-1}}.$$

Durch Wegschaffung der Nenner erhält man hieraus leicht

$$B_k(-BN_k - AZ_k) - A_k(BN_{k-1} + AZ_{k-1})$$
$$+ DN_k + \sqrt{D}\,[B_k N_k + A_k N_{k-1} - (BN_k + AZ_k)] = 0.$$

Diese Gleichung kann nur bestehen, wenn sowohl der

rationale, als auch der irrationale Theil Null ist; wir erhalten somit die beiden Gleichungen

$$(1) \quad -B_k(BN_k + AZ_k) - A_k(BN_{k-1} + AZ_{k-1}) = -DN_k,$$

$$(2) \quad B_k N_k + A_k N_{k-1} = BN_k + AZ_k,$$

durch deren Auflösung sich mit Rücksicht auf die bekannte Formel

$$Z_k N_{k-1} - Z_{k-1} N_k = (-1)^k$$

leicht

$$(3) \quad A_k = \frac{(-1)^k}{A}[(AZ_k + BN_k)^2 - DN_k^2],$$

$$(4) \quad B_k = (-1)^{k+1}[AZ_k Z_{k-1} + B(Z_k N_{k-1} + Z_{k-1} N_k) + CN_k N_{k-1}]$$

ergiebt.

Nun folgt aus (3)

$$A_k = \frac{(-1)^k}{A}(AZ_k + BN_k + N_k\sqrt{D})(AZ_k + BN_k - N_k\sqrt{D}),$$

oder durch Absonderung von N_k^2

$$A_k = \frac{(-1)^k N_k^2}{A}\left(A\frac{Z_k}{N_k} + B + \sqrt{D}\right)\left(A\frac{Z_k}{N_k} + B - \sqrt{D}\right)$$

$$= \frac{(-1)^k N_k^2}{A}\left(A\frac{Z_k}{N_k} + 2\sqrt{D} + B - \sqrt{D}\right)\left(A\frac{Z_k}{N_k} + B - \sqrt{D}\right)$$

$$= (-1)^k N_k^2\left[2\sqrt{D} + A\left(\frac{Z_k}{N_k} - \frac{-B+\sqrt{D}}{A}\right)\right]\left(\frac{Z_k}{N_k} - \frac{-B+\sqrt{D}}{A}\right).$$

Der Factor

$$\frac{Z_k}{N_k} - \frac{-B+\sqrt{D}}{A} = \frac{Z_k}{N_k} - x$$

ist positiv oder negativ, je nachdem k gerade oder ungerade ist, folglich ist das Produkt

$$(-1)^k N_k^2\left(\frac{Z_k}{N_k} - \frac{-B+\sqrt{D}}{A}\right)$$

stets positiv. Was weiter den in den eckigen Klammern enthaltenen Factor betrifft, so nähert sich derselbe, wenn man k wachsen lässt, der positiven Grenze $2\sqrt{D}$, da für wachsende k die Differenz $\frac{Z_k}{N_k} - x$ immer kleiner wird. Es wird

also von einer gewissen Grenze an die Zahl A_k ein Produkt positiver Factoren, mithin selbst positiv sein.

Dass auch B_k positiv ist, sobald k eine gewisse Grenze erreicht hat, folgt aus der Gleichung (2), die wir auch in der Form

$$\frac{N_{k-1}A_k}{N_k} = A\frac{Z_k}{N_k} + B - B_k$$

schreiben können. Dividirt man nämlich die linke Seite durch $A_k x_k$, die rechte durch die gleiche Zahl $B_k + \sqrt{D}$, so folgt

$$\frac{N_{k-1}}{N_k x_k} = \frac{\left(A\frac{Z_k}{N_k} + B\right) - B_k}{B_k + \sqrt{D}},$$

und die linke Seite dieser Formel ist offenbar < 1. Was die rechte Seite betrifft, so ist

$$x = \frac{-B + \sqrt{D}}{A},$$

also

$$Ax + B = \sqrt{D};$$

wenn wir demnach x durch $\frac{Z_k}{N_k}$ ersetzen, so werden wir der positiven Zahl $\sqrt{D}$ um so näher kommen, je mehr wir k wachsen lassen.

Die rechte Seite unserer Formel nähert sich also bei wachsendem k der Grenze $\frac{\sqrt{D} - B_k}{\sqrt{D} + B_k}$, und da dieser Ausdruck < 1 sein soll, so muss B_k eine positive Zahl sein.

§ 41. Periodische Kettenbrüche. Ein unendlicher Kettenbruch heisst periodisch, wenn die Reihe der vollständigen oder unvollständigen Quotienten von einer bestimmten Stelle an in unveränderter Folge wiederkehrt. Die sich in dieser Weise wiederholenden Quotienten bilden die Periode der vollständigen oder unvollständigen Quotienten; die Periode kann ein- oder mehrgliedrig sein. Wenn die Periode gleich mit dem ersten Quotienten beginnt, so heisst der Kettenbruch rein periodisch; wenn ein oder mehrere Glieder der Periode vorangehen, so wird der Kettenbruch unrein periodisch genannt.

Lehrsatz I. Der Kettenbruch, in welchen sich eine irrationale Wurzel einer Gleichung zweiten Grades mit ganzen Coefficienten entwickeln lässt, ist periodisch.

Beweis. Es sei wieder

$$x = \frac{-B + \sqrt{D}}{A}$$

die eine irrationale Wurzel der Gleichung

$$Ax^2 + 2Bx + C = 0,$$

und man habe auf die dargelegte Weise

$$x \quad = a + \frac{1}{x_1},$$

$$x_1 \quad = \frac{B_1 + \sqrt{D}}{A_1} = a_1 + \frac{1}{x_2},$$

$$\cdots\cdots\cdots\cdots,$$

$$x_{k-1} = \frac{B_{k-1} + \sqrt{D}}{A_{k-1}} = a_{k-1} + \frac{1}{x_k},$$

$$\cdots\cdots\cdots\cdots$$

gefunden, wo $A_1, A_2, \ldots, B_1, B_2, \ldots$ ganze und für alle über eine gewisse Grenze hinausliegenden Werthe von k positive Zahlen sind. Auf solche Werthe von k sollen sich die nachstehenden Entwicklungen beziehen.

Es ist

$$x_{k-1} = \frac{B_{k-1} + \sqrt{D}}{A_{k-1}} = a_{k-1} + \frac{1}{x_k},$$

also

$$x_k = \frac{A_{k-1}}{\sqrt{D} + B_{k-1} - a_{k-1} A_{k-1}}$$

$$= \frac{\sqrt{D} + a_{k-1} A_{k-1} - B_{k-1}}{\frac{1}{A_{k-1}} [D - (a_{k-1} A_{k-1} - B_{k-1})^2]}.$$

Dieser Ausdruck soll $= \frac{B_k + \sqrt{D}}{A_k}$ sein; man hat daher

$$(1) \qquad B_k = a_{k-1} A_{k-1} - B_{k-1},$$

$$(2) \qquad A_k = \frac{1}{A_{k-1}} [D - (a_{k-1} A_{k-1} - B_{k-1})^2].$$

Wenn man aus jeder dieser Gleichungen

$$(a_{k-1} A_{k-1} - B_{k-1})^2$$

berechnet und die erhaltenen Werthe einander gleich setzt, so ergiebt sich

(3) $$B_k^2 = D - A_{k-1} A_k,$$

und daraus folgt zunächst, dass

$$B_k < \sqrt{D}$$

ist; dann geht aber aus (1) hervor, wenn darin k statt $k-1$ geschrieben wird, dass

$$A_k < 2\sqrt{D}, \quad a_k < 2\sqrt{D}$$

ist. Die positiven ganzen Zahlen a_k, A_k, B_k sind somit in Grenzen eingeschlossen, und daher muss nach höchstens

$$2\sqrt{D} \,.\, \sqrt{D} = 2D$$

Operationen ein vollständiger Quotient auftreten, der mit einem vorausgegangenen identisch ist.

Lehrsatz II. (Umkehrung). Jede Grösse, die sich in einen periodischen Kettenbruch entwickeln lässt, ist Wurzel einer Gleichung zweiten Grades mit ganzen Coefficienten.

Beweis. Der Kettenbruch sei zunächst rein periodisch, und die Periode seiner unvollständigen Quotienten bestehe aus den k Gliedern $a, a_1, a_2, \ldots, a_{k-1}$, so dass wieder

$$a_k = a, \quad a_{k+1} = a_1, \ldots$$

ist. Dann ist

$$x_k = x,$$

und die Formel

$$x = \frac{Z_k x_k + Z_{k-1}}{N_k x_k + N_{k-1}}$$

geht, wenn x_k durch x ersetzt wird, über in

$$x = \frac{Z_k x + Z_{k-1}}{N_k x + N_{k-1}},$$

woraus sich die Gleichung zweiten Grades

$$N_k x^2 + (N_{k-1} - Z_k)x - Z_{k-1} = 0$$

ergiebt.

Zweitens sei der Kettenbruch unrein periodisch, und zwar mögen der wieder aus k Gliedern bestehenden Periode noch die m unvollständigen Quotienten $a, a_1, a_2, \ldots, a_{m-1}$ vorangehen. Dann ist $x_{m+k} = x_m$.

Nun hat man

$$x = \frac{Z_m x_m + Z_{m-1}}{N_m x_m + N_{m-1}},$$

folglich

$$x_m = \frac{N_{m-1} x - Z_{m-1}}{Z_m - N_m x},$$

und

$$x = \frac{Z_{m+k} x_{m+k} + Z_{m+k-1}}{N_{m+k} x_{m+k} + N_{m+k-1}},$$

folglich

$$x_{m+k} = \frac{N_{m+k-1} x - Z_{m+k-1}}{Z_{m+k} - N_{m+k} x};$$

somit ist

$$\frac{N_{m-1} x - Z_{m-1}}{Z_m - N_m x} = \frac{N_{m+k-1} x - Z_{m+k-1}}{Z_{m+k} - N_{m+k} x},$$

und auch diese Gleichung wird durch Fortschaffung der Nenner eine quadratische Gleichung mit ganzen Coefficienten.

Lehrsatz III. Entwickelt man die irrationalen Wurzeln einer Gleichung zweiten Grades in Kettenbrüche, so ist die Periode der unvollständigen Quotienten des einen die Umkehrung der Periode des andern.

Beweis. Wir setzen die Wurzel x, die wir in einen Kettenbruch entwickeln, als positiv und > 1 voraus, was zulässig ist, da wir, wenn x negativ ist, es durch $-x$, und wenn $x < 1$ ist, es durch $+\frac{1}{x}$ ersetzen können, so dass das neue x den gestellten Anforderungen genügt. Es ist dann

$$x = \frac{Z_k x_k + Z_{k-1}}{N_k x_k + N_{k-1}},$$

also

$$x_k = \frac{N_{k-1} x - Z_{k-1}}{Z_k - N_k x}.$$

Wenn nun der Kettenbruch zunächst rein periodisch ist, so ist, falls die Periode aus k Gliedern besteht, $x = x_k$, und wir erhalten wieder die Gleichung, deren eine Wurzel x ist, wenn wir in einer der beiden vorstehenden Formeln x_k durch x ersetzen; diese Gleichung ist also

$$x = \frac{N_{k-1} x - Z_{k-1}}{Z_k - N_k x}.$$

Die zweite Wurzel dieser Gleichung ist negativ; wird dieselbe mit $-\frac{1}{x'}$ bezeichnet, so ist

$$-\frac{1}{x'} = \frac{-\frac{N_{k-1}}{x'} - Z_{k-1}}{Z_k + \frac{N_k}{x'}},$$

woraus leicht

$$x' = \frac{Z_k x' + N_k}{Z_{k-1} x' + N_{k-1}}$$

folgt. Hieraus geht zunächst hervor, dass in der Reihe der unvollständigen Quotienten der Entwicklung von x'

$$b, b_1, b_2, \ldots b_{k-1}, \ldots$$

das $(k+1)^{\text{te}}$ Glied $b_k = b$ sein wird, u. s. w. Nun sahen wir oben in § 37, dass, wenn ein Bruch $\frac{Z_k}{N_k}$ die unvollständigen Quotienten $a, a_1, a_2, \ldots, a_{k-1}$ liefert, der Bruch $\frac{Z_k}{Z_{k-1}}$ die unvollständigen Quotienten $a_{k-1}, a_{k-2}, \ldots, a_1, a$ liefern wird. Folglich ist der Kettenbruch, welchen x' liefert, gleichfalls periodisch, seine Periode besteht aus k Gliedern und ist die Umkehrung der Periode von x. Der $(k-1)^{\text{te}}$ Näherungsbruch von x' ist $\frac{N_k}{N_{k-1}}$.

Zweitens nehmen wir an, der Kettenbruch, welchen die positive Wurzel x liefert, sei unrein periodisch, und zwar beginne die Periode, die aus k Gliedern bestehen möge, mit dem $(m+1)^{\text{ten}}$ Quotienten; dann ist

$$x = \frac{Z_m x_m + Z_{m-1}}{N_m x_m + N_{m-1}}.$$

Nun wird x_m sich in einen rein periodischen Kettenbruch entwickeln lassen, also Wurzel einer quadratischen Gleichung sein, und wenn $-\frac{1}{x_m'}$ die zweite (negative) Wurzel dieser Gleichung bezeichnet, so wird auch x_m' einen rein periodischen Kettenbruch liefern, dessen Periode die Umkehrung der Periode von x_m ist. Wir erhalten also die zweite Wurzel x' der vor-

gelegten Gleichung, wenn wir in der vorhergehenden Formel x_m durch $-\frac{1}{x'_m}$ ersetzen, d. h. es ist

$$x' = \frac{Z_{m-1} x'_m - Z_m}{N_{m-1} x'_m - N_m}.$$

Die Kettenbrüche, die sich für x' und x'_m ergeben, haben, da

$$Z_m N_{m-1} - N_m Z_{m-1} = (-1)^m$$

ist, einen vollständigen Quotienten gemeinsam. Dieser möge den unvollständigen Quotienten a_λ liefern; dann ist a_λ, weil der Entwicklung von x'_m angehörig, auch ein unvollständiger Quotient von x_m und somit auch von x, und zwar muss $\lambda < k - 1$ sein. Ist nun

$$a,\ a_1,\ a_2,\ \ldots,\ a_\lambda,\ \ldots,\ a_{k-1}$$

die Periode von x, also

$$a_{k-1},\ a_{k-2},\ \ldots,\ a_\lambda,\ \ldots,\ a_2,\ a_1,\ a$$

die von x'_m, so dürfen wir auch, da wir die Periode eines Bruches mit jedem Quotienten der Periode beginnen können,

$$a_{\lambda+1},\ a_{\lambda+2},\ \ldots\ a_{k-1},\ a,\ a_1,\ a_2,\ \ldots,\ a_\lambda$$

als Periode von x und

$$a_\lambda,\ a_{\lambda-1},\ \ldots,\ a_2,\ a_1,\ a,\ a_{k-1},\ \ldots,\ a_{\lambda+1}$$

als Periode von x' annehmen. Die Periode von x' kann also als die Umkehrung der Periode von x angesehen werden.

So fanden wir oben für die Wurzel

$$x = \frac{7 + \sqrt{19}}{3}$$

der Gleichung

$$3x^2 - 14x + 10 = 0$$

die unvollständigen Quotienten

$$3,\ (1,\ 3,\ 1,\ 2,\ 8,\ 2),\ \ldots,$$

und für die zweite Wurzel

$$x' = \frac{7 - \sqrt{19}}{3}$$

$$0,\ 1,\ 7,\ (2,\ 1,\ 3,\ 1,\ 2,\ 8),\ \ldots;$$

damit die Periode der letzteren die Umkehrung der Periode von x sei, müssen wir sie mit dem 8ten Quotienten beginnen, also

$$0,\ 1,\ 7,\ 2,\ 1,\ 3,\ 1,\ (2,\ 8,\ 2,\ 1,\ 3,\ 1),\ \ldots$$

schreiben.

Aufgaben. I. Die Wurzeln der Gleichung

$$3x^2 - 10x - 28 = 0$$

in Kettenbrüche zu entwickeln.

1. Wurzel. $x = \frac{5 + \sqrt{109}}{3}$

$$x = \frac{5 + \sqrt{109}}{3} = 5 + \frac{-10 + \sqrt{109}}{3} = 5 + \frac{1}{x_1}$$

$$x_1 = \frac{10 + \sqrt{109}}{3} = 6 + \frac{-8 + \sqrt{109}}{3} = 6 + \frac{1}{x_2}$$

$$x_2 = \frac{8 + \sqrt{109}}{15} = 1 + \frac{-7 + \sqrt{109}}{15} = 1 + \frac{1}{x_3}$$

$$x_3 = \frac{7 + \sqrt{109}}{4} = 4 + \frac{-9 + \sqrt{109}}{4} = 4 + \frac{1}{x_4}$$

$$x_4 = \frac{9 + \sqrt{109}}{7} = 2 + \frac{-5 + \sqrt{109}}{7} = 2 + \frac{1}{x_5}$$

$$x_5 = \frac{5 + \sqrt{109}}{12} = 1 + \frac{-7 + \sqrt{109}}{12} = 1 + \frac{1}{x_6}$$

$$x_6 = \frac{7 + \sqrt{109}}{5} = 3 + \frac{-8 + \sqrt{109}}{5} = 3 + \frac{1}{x_7}$$

$$x_7 = \frac{8 + \sqrt{109}}{9} = 2 + \frac{-10 + \sqrt{109}}{9} = 2 + \frac{1}{x_8}$$

$$x_8 = \frac{10 + \sqrt{109}}{1} = 20 + \frac{-10 + \sqrt{109}}{1} = 20 + \frac{1}{x_9}$$

$$x_9 = \frac{10 + \sqrt{109}}{9} = 2 + \frac{-8 + \sqrt{109}}{9} = 2 + \frac{1}{x_{10}}$$

$$x_{10} = \frac{8 + \sqrt{109}}{5} = 3 + \frac{-7 + \sqrt{109}}{5} = 3 + \frac{1}{x_{11}}$$

$$x_{11} = \frac{7 + \sqrt{109}}{12} = 1 + \frac{-5 + \sqrt{109}}{12} = 1 + \frac{1}{x_{12}}$$

$$x_{12} = \frac{5 + \sqrt{109}}{7} = 2 + \frac{-9 + \sqrt{109}}{7} = 2 + \frac{1}{x_{13}}$$

$$x_{13} = \frac{9 + \sqrt{109}}{4} = 4 + \frac{-7 + \sqrt{109}}{4} = 4 + \frac{1}{x_{14}}$$

$$x_{14} = \frac{7 + \sqrt{109}}{15} = 1 + \frac{-8 + \sqrt{109}}{15} = 1 + \frac{1}{x_{15}}$$

$$x_{15} = \frac{8 + \sqrt{109}}{3} = 6 + \frac{-10 + \sqrt{109}}{3} = 6 + \frac{1}{x_1}.$$

2. Wurzel. Absoluter Werth $x' = \frac{-5 + \sqrt{109}}{3}$.

$$x' = \frac{-5+\sqrt{109}}{3} = 1 + \frac{-8+\sqrt{109}}{3} = 1 + \frac{1}{x_1'},$$

$$x_1' = \frac{8+\sqrt{109}}{15} = 1 + \frac{-7+\sqrt{109}}{15} = 1 + \frac{1}{x_2'},$$

$$x_2' = \frac{7+\sqrt{109}}{4} = 4 + \frac{-9+\sqrt{109}}{4} = 4 + \frac{1}{x_3'},$$

$$x_3' = \frac{9+\sqrt{109}}{7} = 2 + \frac{-5+\sqrt{109}}{7} = 2 + \frac{1}{x_4'},$$

$$x_4' = \frac{5+\sqrt{109}}{12} = 1 + \frac{-7+\sqrt{109}}{12} = 1 + \frac{1}{x_5'},$$

$$x_5' = \frac{7+\sqrt{109}}{5} = 3 + \frac{-8+\sqrt{109}}{5} = 3 + \frac{1}{x_6'},$$

$$x_6' = \frac{8+\sqrt{109}}{9} = 2 + \frac{-10+\sqrt{109}}{9} = 2 + \frac{1}{x_7'},$$

$$x_7' = \frac{10+\sqrt{109}}{1} = 20 + \frac{-10+\sqrt{109}}{1} = 20 + \frac{1}{x_8'},$$

$$x_8' = \frac{10+\sqrt{109}}{9} = 2 + \frac{-8+\sqrt{109}}{9} = 2 + \frac{1}{x_9'},$$

$$x_9' = \frac{8+\sqrt{109}}{5} = 3 + \frac{-7+\sqrt{109}}{5} = 3 + \frac{1}{x_{10}'}$$

$$x_{10}' = \frac{7+\sqrt{109}}{12} = 1 + \frac{-5+\sqrt{109}}{12} = 1 + \frac{1}{x_{11}'}$$

$$x_{11}' = \frac{5+\sqrt{109}}{7} = 2 + \frac{-9+\sqrt{109}}{7} = 2 + \frac{1}{x_{12}'}$$

$$x_{12}' = \frac{9+\sqrt{109}}{4} = 4 + \frac{-7+\sqrt{109}}{4} = 4 + \frac{1}{x_{13}'}$$

$$x_{13}' = \frac{7+\sqrt{109}}{15} = 1 + \frac{-8+\sqrt{109}}{15} = 1 + \frac{1}{x_{14}'}$$

$$x_{14}' = \frac{8+\sqrt{109}}{3} = 6 + \frac{-10+\sqrt{109}}{3} = 6 + \frac{1}{x_{15}'}$$

$$x_{15}' = \frac{10+\sqrt{109}}{3} = 6 + \frac{-8+\sqrt{109}}{3} = 6 + \frac{1}{x_1'}.$$

II. Welche Gleichung hat den unendlichen periodischen Kettenbruch

$$3 + \cfrac{1}{7 + \cfrac{1}{4 + \cfrac{1}{7 + \cdots}}}$$

zur Wurzel?

Es ist

$$x - 3 = \frac{1}{7 + \frac{1}{4 + (x - 3)}},$$

und daraus folgt leicht

$$7x^2 - 14x = 25.$$

§ 42. Entwicklung einer irrationalen Quadratwurzel in einen Kettenbruch. — Von besonderem Interesse ist es, die Grösse $\sqrt{A}$ in einen Kettenbruch zu entwickeln. Auch hier wollen wir zunächst an einem Beispiel den Gang der Rechnung zeigen. Es ist

$$\sqrt{69} = 8 + \frac{-8 + \sqrt{69}}{1} = 8 + \frac{1}{x_1}$$

$$x_1 = \frac{8 + \sqrt{69}}{5} = 3 + \frac{-7 + \sqrt{69}}{5} = 3 + \frac{1}{x_2}$$

$$x_2 = \frac{7 + \sqrt{69}}{4} = 3 + \frac{-5 + \sqrt{69}}{4} = 3 + \frac{1}{x_3}$$

$$x_3 = \frac{5 + \sqrt{69}}{11} = 1 + \frac{-6 + \sqrt{69}}{11} = 1 + \frac{1}{x_4}$$

$$x_4 = \frac{6 + \sqrt{69}}{3} = 4 + \frac{-6 + \sqrt{69}}{3} = 4 + \frac{1}{x_5}$$

$$x_5 = \frac{6 + \sqrt{69}}{11} = 1 + \frac{-5 + \sqrt{69}}{11} = 1 + \frac{1}{x_6}$$

$$x_6 = \frac{5 + \sqrt{69}}{4} = 3 + \frac{-7 + \sqrt{69}}{4} = 3 + \frac{1}{x_7}$$

$$x_7 = \frac{7 + \sqrt{69}}{5} = 3 + \frac{-8 + \sqrt{69}}{5} = 3 + \frac{1}{x_8}$$

$$x_8 = \frac{8 + \sqrt{69}}{1} = 16 + \frac{-8 + \sqrt{69}}{1} = 16 + \frac{1}{x_1}.$$

Der erste unvollständige Quotient, den wir erhalten, ist also die in $\sqrt{A}$ enthaltene grösste ganze Zahl a. Wir setzen dann

$$\sqrt{A} = a + \frac{-a + \sqrt{A}}{1} = a + \frac{1}{x_1},$$

wo $x_1 = \frac{1}{-a + \sqrt{A}}$ ist. Den Nenner dieses Bruches machen wir durch Erweiterung mit $a + \sqrt{A}$ rational und erhalten

$$x_1 = \frac{a + \sqrt{A}}{b},$$

wo $b = A - a^2$, also eine ganze Zahl ist. Mit x_1 verfahren wir dann genau in der oben in § 40 dargelegten Weise.

Der Kettenbruch, zu dem wir gelangen, hat nun folgende Eigenschaften:

1. Derselbe ist periodisch, da $\sqrt{A}$ eine Wurzel der Gleichung $x^2 - A = 0$ ist.

2. Derselbe kann nicht rein periodisch sein; denn ein solcher Kettenbruch führt zu der Gleichung

$$N_k x^2 + (N_{k-1} - Z_k)x - Z_{k-1} = 0$$

(vgl. § 41, Lehrsatz II), und damit diese rein quadratisch werde, muss $N_{k-1} - Z_k = 0$ sein. Dann geht aber die bekannte Formel

$$Z_k N_{k-1} - N_k Z_{k-1} = (-1)^k$$

über in

$$Z_k^2 = N_k Z_{k-1} + (-1)^k$$

und liefert

$$\frac{Z_k}{N_k} = \frac{Z_{k-1}}{Z_k} + \frac{(-1)^k}{Z_k N_k}.$$

Das ist unmöglich, da ein Näherungsbruch von $\sqrt{A}$ nicht < 1 sein kann.

3. Der Periode können nicht mehrere Glieder vorausgehen. Dies zu beweisen, nehmen wir an, der aus k Gliedern bestehenden Periode der unvollständigen Quotienten gingen m Glieder voraus; dann besteht die für diesen Fall in § 41 Lehrsatz II hergeleitete Gleichung, welche, geordnet, die Form

$$Ax^2 + Bx + C = 0$$

hat, wo

$$A = N_m N_{m+k-1} - N_{m-1} N_{m+k},$$
$$B = N_{m-1} Z_{m+k} + Z_{m-1} N_{m+k} - Z_m N_{m+k-1} - N_m Z_{m+k-1},$$
$$C = Z_m Z_{m+k-1} - Z_{m-1} Z_{m+k}$$

ist. Das Produkt der Wurzeln dieser Gleichung ist bekanntlich

$$P = \frac{C}{A} = \frac{Z_m Z_{m+k-1} - Z_{m-1} Z_{m+k}}{N_m N_{m+k-1} - N_{m-1} N_{m+k}},$$

oder, wenn

$$Z_m = a_{m-1} Z_{m-1} + Z_{m-2},$$
$$N_m = a_{m-1} N_{m-1} + N_{m-2},$$

$$Z_{m+k} = a_{m+k-1} Z_{m+k-1} + Z_{m+k-2},$$
$$N_{m+k} = a_{m+k-1} N_{m+k-1} + N_{m+k-2},$$

gesetzt wird,

$$P = \frac{(a_{m-1} Z_{m-1} + Z_{m-2}) Z_{m+k-1} - Z_{m-1}(a_{m+k-1} Z_{m+k-1} + Z_{m+k-2})}{(a_{m-1} N_{m-1} + N_{m-2}) N_{m+k-1} - N_{m-1}(a_{m+k-1} N_{m+k-1} + N_{m+k-2})}$$

$$= \frac{Z_{m-1} Z_{m+k-1}}{N_{m-1} N_{m+k-1}} \cdot \frac{(a_{m-1} - a_{m+k-1}) + \left(\frac{Z_{m-2}}{Z_{m-1}} - \frac{Z_{m+k-2}}{Z_{m+k-1}}\right)}{(a_{m-1} - a_{m+k-1}) + \left(\frac{N_{m-2}}{N_{m-1}} - \frac{N_{m+k-2}}{N_{m+k-1}}\right)}.$$

Da a_{m-1} von a_{m+k-1} verschieden ist (sonst würde die Periode schon eine Stelle früher, als vorausgesetzt wurde, beginnen), so ist $a_{m-1} - a_{m+k-1}$ eine von Null verschiedene ganze Zahl. Ferner ist sowohl

$$\frac{Z_{m-2}}{Z_{m-1}} - \frac{Z_{m+k-2}}{Z_{m+k-1}},$$

als auch

$$\frac{N_{m-2}}{N_{m-1}} - \frac{N_{m+k-2}}{N_{m+k-1}}$$

ein echter Bruch. Daher ist P eine positive Grösse, und da die Wurzeln der Gleichung $x^2 - A = 0$ ein negatives Produkt haben, so ist bewiesen, dass der Periode der unvollständigen Quotienten des Kettenbruchs, welcher $\sqrt{A}$ darstellt, nicht mehrere Glieder vorausgehen können.

4. Der Periode geht also immer **ein** Glied voraus. In der That ist, wenn $m = 1$ angenommen wird,

$$Z_m = a, \quad N_m = 1, \quad Z_{m-1} = 1, \quad N_{m-1} = 0,$$

und dann wird

$$P = \frac{a Z_k - Z_{k+1}}{N_k},$$

welche Zahl sowohl positiv, als negativ sein kann.

5. Wenn a die grösste in $\sqrt{A}$ enthaltene ganze Zahl bezeichnet, so ist das letzte Glied der Periode $= 2a$, und die übrigen Glieder bilden eine symmetrische Reihe, d. h. die von den Enden gleich weit entfernten Glieder sind einander gleich.

Da nämlich $\sqrt{A}$ einen Kettenbruch liefert, dessen Periode mit dem zweiten unvollständigen Quotienten beginnt, so

wird die Entwicklung von $\sqrt{A} - a$ einen rein periodischen Kettenbruch geben. Dasselbe ist dann mit $\sqrt{A} + a$ der Fall, denn $-(\sqrt{A} - a)$ und $(\sqrt{A} + a)$ sind die Wurzeln der Gleichung

$$x^2 - 2ax + (a^2 - A) = 0.$$

Ist nun

$$(2a, a_1, a_2, \ldots, a_{k-1})$$

die Periode des Kettenbruchs, der gleich $\sqrt{A} + a$ ist, so werden die unvollständigen Quotienten für $\sqrt{A} - a$ nach § 41, Lehrsatz III folgende sein:

$$0, (a_{k-1}, a_{k-2}, \ldots, a_2, a_1, 2a), (a_{k-1}, \ldots), \ldots$$

Aus dem ersteren Kettenbruch folgt der Kettenbruch $\sqrt{A}$, indem wir den ersten unvollständigen Quotienten, d. i. $2a$, um a vermindern; aus dem zweiten ergiebt sich derselbe, wenn wir den ersten unvollständigen Quotienten, d. i. 0, um a vermehren. Beide Resultate müssen zusammenfallen; es sind also die Reihen der unvollständigen Quotienten

$$a, (a_1, a_2, \ldots, a_{k-1}, 2a), (a_1, \ldots$$
$$a, (a_{k-1}, a_{k-2}, \ldots, a_1, 2a), (a_{k-1}, \ldots$$

identisch; daher ist das letzte Glied der Periode $2a$, und die übrigen Glieder bilden eine symmetrische Reihe.

Aufgaben. I. $\sqrt{29}$ in einen Kettenbruch zu verwandeln.

$$\sqrt{29} = 5 + \frac{-5 + \sqrt{29}}{1} = 5 + \frac{1}{x_1}$$

$$x_1 = \frac{5 + \sqrt{29}}{4} = 2 + \frac{-3 + \sqrt{29}}{4} = 2 + \frac{1}{x_2}$$

$$x_2 = \frac{3 + \sqrt{29}}{5} = 1 + \frac{-2 + \sqrt{29}}{5} = 1 + \frac{1}{x_3}$$

$$x_3 = \frac{2 + \sqrt{29}}{5} = 1 + \frac{-3 + \sqrt{29}}{5} = 1 + \frac{1}{x_4}$$

$$x_4 = \frac{3 + \sqrt{29}}{4} = 2 + \frac{-5 + \sqrt{29}}{4} = 2 + \frac{1}{x_5}$$

$$x_5 = \frac{5 + \sqrt{29}}{1} = 10 + \frac{-5 + \sqrt{29}}{1} = 10 + \frac{1}{x_1}.$$

II. Welche Quadratwurzel stellt der unendliche periodische Kettenbruch dar, dessen unvollständige Quotienten

$$4,\ (2,\ 1,\ 3,\ 1,\ 2,\ 8),\ (2,\ 1, \ldots$$

sind?

Wird der Werth des Kettenbruchs mit x bezeichnet, so ist $x - 4$ ein rein periodischer Kettenbruch, dessen Werth dadurch erhalten wird, dass man in dem Näherungsbruch, welcher dem unvollständigen Quotienten 8 entspricht, 8 durch

$$8 + x - 4 = x + 4$$

ersetzt. Die Rechnung gestaltet sich also folgendermassen:

0	2	1	3	1	2	$x+4$	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{4}{11}$	$\frac{5}{14}$	$\frac{14}{39}$	$\frac{14(x+4)+5}{39(x+4)+14}$.

Es ist somit

$$x - 4 = \frac{14(x+4) + 5}{39(x+4) + 14},$$

und daraus folgt leicht

$$x = \sqrt{19}.$$

§ 43. Auflösung der Pell'schen Gleichung. — Wenn $\frac{\alpha_m + \sqrt{A}}{\beta_m}$ einer der vollständigen Quotienten ist, welche die Entwicklung von $\sqrt{A}$ in einen Kettenbruch liefert, und a_m den zugehörigen unvollständigen Quotienten bezeichnet, so haben wir nach dem Früheren

$$\frac{\alpha_m + \sqrt{A}}{\beta_m} = a_m + \frac{(\alpha_m - a_m \beta_m) + \sqrt{A}}{\beta_m} = a_m + \frac{1}{x_{m+1}}$$

zu setzen, wo

$$x_{m+1} = \frac{(-\alpha_m + a_m \beta_m) + \sqrt{A}}{\frac{1}{\beta_m}[A - (\alpha_m - a_m \beta_m)^2]} = \frac{\alpha_{m+1} + \sqrt{A}}{\beta_{m+1}}$$

ist. Es ist daher

$$\alpha_{m+1} = -\alpha_m + a_m \beta_m$$

und

$$A - \alpha_{m+1}^2 = \beta_m \beta_{m+1}.$$

Daraus geht hervor, dass in jedem vollständigen Quotienten $\frac{\alpha + \sqrt{A}}{\beta}$ die Zahl $\alpha < \sqrt{A}$, also $\leqq a$ ist, wo a die grösste in $\sqrt{A}$ enthaltene ganze Zahl bezeichnet.

Nun schliesst die Periode der unvollständigen Quotienten, die wieder aus k Gliedern bestehen möge, mit $2a$, und damit die grösste in dem vollständigen Quotienten $\frac{\alpha_k + \sqrt{A}}{\beta_k}$ enthaltene ganze Zahl diesen Werth habe, muss danach

$$\alpha_k = a\,, \quad \beta_k = 1$$

sein. Dem letzten unvollständigen Quotienten $2a$ jeder Periode entspricht somit der vollständige Quotient

$$x_k = \frac{a + \sqrt{A}}{1}\,.$$

Für diesen Werth von x_k geht die oft benutzte Formel

$$x = \frac{Z_k x_k + Z_{k-1}}{N_k x_k + N_{k-1}}$$

über in

$$\sqrt{A} = \frac{Z_k (a + \sqrt{A}) + Z_{k-1}}{N_k (a + \sqrt{A}) + N_{k-1}}\,.$$

Durch Fortschaffung des Nenners und durch Gleichsetzung der rationalen und der irrationalen Theile beider Seiten erhält man hieraus die beiden Gleichungen

$$a N_k = Z_k - N_{k-1}$$

$$a Z_k = A N_k - Z_{k-1}\,,$$

aus denen sich durch Elimination von a

$$Z_k^2 - A N_k^2 = Z_k N_{k-1} - N_k Z_{k-1}$$

oder, da $Z_k N_{k-1} - N_k Z_{k-1} = (-1)^k$ ist,

$$Z_k^2 - A N_k^2 = (-1)^k$$

ergiebt.

Diese Formel löst, wie wir sehen werden, die Gleichung

$$x^2 - A y^2 = 1\,,$$

zu deren Lösung Fermat die englischen Mathematiker herausgefordert hatte. Die von Pell (daher Pell'sche Gleichung) daraufhin gegebene Lösung, welche den Inhalt des Kap. 7 von Euler's Algebra Bd. II bildet, hat nicht nur den Nachtheil, meist ungemein langwierig zu sein, sondern sie lässt auch nicht erkennen, dass die Aufgabe immer möglich ist, d. h. dass es ausser der auf der Hand liegenden Lösung

$$x = \pm 1\,, \quad y = 0$$

noch andere Lösungen in ganzen Zahlen giebt. „Erst Lagrange hat diesen Beweis geführt (Abhandlungen der Berliner Akademie, 1767), und dieser Beweis, wie auch die Auflösungsmethode, die ihn begleitet, können als einer der grössten Fortschritte angesehen werden, welche die Zahlentheorie zu verzeichnen hat; denn die Gleichung

$$x^2 - Ay^2 = 1$$

ist nicht nur an sich sehr interessant, sondern sie ist auch nothwendig bei der Auflösung aller unbestimmten Gleichungen zweiten Grades, wo sie dazu dient, eine unendliche Menge von Lösungen zu finden, wenn eine einzige bekannt ist.“ (Legendre).

Nach Lagrange lösen wir nun die Gleichung

$$x^2 - Ay^2 = 1\,, \tag{1}$$

in welcher A positiv und keine Quadratzahl ist, auf folgende Weise:

Wir entwickeln $\sqrt{A}$ in einen Kettenbruch und bilden die Reihe der Näherungsbrüche. Dann entspricht dem letzten unvollständigen Quotienten der ersten Periode der Näherungsbruch $\frac{Z_k}{N_k}$, dem letzten Gliede der zweiten Periode $\frac{Z_{2k}}{N_{2k}}$, u. s. w., dem letzten Gliede der μ^{ten} Periode $\frac{Z_{\mu k}}{N_{\mu k}}$, und es ist, wie wir oben gefunden haben, allgemein

$$Z_{\mu k}^2 - AN_{\mu k}^2 = (-1)^{\mu k}. \tag{2}$$

Wenn nun die Anzahl k der Glieder einer Periode gerade ist, so ist die rechte Seite dieser Gleichung für jeden Werth von μ gleich $+1$, also hat die Gleichung (1) die unendlich vielen Lösungen

$$x = Z,\quad y = N,$$

wo Z der Zähler und N der zugehörige Nenner jedes der unendlich vielen Näherungsbrüche ist, welche dem letzten Gliede jeder der Perioden entsprechen.

Ist dagegen k eine ungerade Zahl, so ist die rechte Seite von (2) nur für gerade Werthe von μ gleich $+1$. In diesem Falle liefern also nur die Näherungsbrüche, welche dem letzten Gliede der zweiten, der vierten, u. s. w. Periode entsprechen, Lösungen der Gleichung (1).

Beispiele. I. $x^2 - 13y^2 = 1$.

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cdots}}}}}}$$

$k = 5$ (ungerade)

3	1	1	1	1	6	1	1	1	1	6
1	3	4	7	11	18	119	137	256	393	649
0	1	1	2	3	5	33	38	71	109	180

Es ist also $x = 649$, $y = 180$ eine der unendlich vielen Lösungen.

Für $x = 18$, $y = 5$ würde $x^2 - 13y^2 = -1$ sein.

II. $x^2 - 38y^2 = 1$.

$$\sqrt{38} = 6 + \cfrac{1}{6 + \cfrac{1}{12 + \cfrac{1}{6 + \cdots}}}$$

$k = 2$ (gerade)

6	6	12	...
1	6	37	...
0	1	6	

$$x = 37, \qquad y = 6$$

eine der unendlich vielen Lösungen.

Anmerkung. Die Gleichung

$$x^2 - Ay^2 = -1$$

ist nur möglich, wenn die Periode der Kettenbruch-Entwicklung von $\sqrt{A}$ aus einer ungeraden Anzahl von Gliedern besteht. In diesem Falle liefern die Näherungsbrüche, welche dem letzten Gliede der ersten, der dritten, u. s. w. Periode entsprechen, Lösungen der Gleichung, wie schon in Beispiel I angedeutet ist.

Uebrigens werden wir uns mit der allgemeinen Pell'schen Gleichung weiter unten noch eingehend zu beschäftigen haben. Hier haben wir dieselbe (für einen speciellen Fall) nur deshalb gelöst, um eine interessante Anwendung der Kettenbruch-Entwicklung einer irrationalen Quadratwurzel zu geben.

Fünftes Kapitel.

Potenzreste für Primzahlmoduln.

§ 44. Berechnung der Potenzreste. — Wir wollen im Folgenden die Reste der successiven Potenzen einer Zahl a für einen Modul p betrachten, der eine in a nicht aufgehende ungerade Primzahl ist. Was die Berechnung der Reste dieser Potenzen

$$1,\ a,\ a^2,\ a^3,\ \ldots$$

betrifft, so hat man nicht nöthig, die Potenzen selbst zu bestimmen. Man erhält nämlich den Rest von a^{m+1}, indem man den Rest von a^m mit a multiplicirt und den Rest des Produkts nimmt. Die folgende Tabelle giebt die Reste der Potenzen der Zahlen von 2 bis 12 für den Modul 13, und zwar bricht die Reihe der Reste jedesmal ab, wenn der Rest 1 erscheint.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
2	4	8	3	6	12	11	9	5	10	7	1
3	9	1									
4	3	12	9	10	1						
5	12	8	1								
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1								
9	3	1									
10	9	12	3	4	1						
11	4	5	3	7	12	2	9	8	10	6	1
12	1										

§ 45. Der Exponent, zu welchem eine Zahl a für den Modul p gehört.

Lehrsatz. Unter den p ersten Gliedern der Reihe

(1) $$1,\ a,\ a^2,\ \ldots;\ a^{p-1},\ \ldots$$

befindet sich ausser der Zahl 1 wenigstens noch ein Glied, welches für den Modul p den Rest 1 hat.

Beweis. Da a nicht durch p theilbar ist, so kann auch keine Potenz von a durch p theilbar sein, d. h. kein Glied von (1) kann den Rest 0 liefern. Die Reste der Potenzen (1) müssen also Zahlen der Reihe

(2) $$1,\ 2,\ 3,\ \ldots,\ (p-1)$$

sein. Unter den p ersten Gliedern von (1) werden sich daher jedenfalls zwei verschiedene Potenzen a^k und a^{k+n} befinden, welche denselben Rest liefern, so dass

$$a^{k+n} \equiv a^k \pmod{p}$$

ist. Diese Congruenz darf, da a^k prim zu p ist, durch a^k dividirt werden und geht dann über in

$$a^n \equiv 1 \pmod{p},$$

wo n kleiner als p ist.

Es giebt also zwischen 1 und p wenigstens eine Zahl n, für welche $a^n \equiv 1 \pmod{p}$ ist. Möglicher Weise sind mehrere Zahlen von dieser Beschaffenheit zwischen 1 und p vorhanden. Die kleinste Zahl n, für welche $a^n \equiv 1 \pmod{p}$ ist, nennt man den Exponenten, zu welchem a für den Modul p gehört. So z. B. gehören, wie die vorstehende Tabelle erkennen lässt, für den Modul 13

die	Zahlen	2, 6, 7, 11	zum	Exponenten	12,
"	"	4, 10	"	"	6,
"	"	5, 8	"	"	4,
"	"	3, 9	"	"	3,
"	Zahl	12	"	"	2.

§ 46. Periodicität der Reihe der Potenzreste.

Lehrsatz I. Gehört die Zahl a für den Modul p zum Exponenten n, so sind die Potenzen $1, a, a^2, \ldots, a^{n-1}$ incongruent.

Beweis. Es seien k und $i = k + r$ Zahlen, die kleiner als n sind (natürlich ist dann auch $r < n$). Hätte man nun

$a^k \equiv a^i \pmod{p}$, so würde sich durch Division mit a^k ergeben, dass $a^r \equiv 1 \pmod{p}$ sein müsste, was der Voraussetzung, nach welcher a zum Exponenten n gehört, widerspricht.

Lehrsatz II. Gehört die Zahl a für den Modul p zum Exponenten n, so ist jede Potenz von a^n auch $\equiv 1 \pmod{p}$ und umgekehrt: Wenn eine Potenz von a den Rest 1 liefert, so muss ihr Exponent ein Vielfaches von n sein.

Beweis. Dass $a^{kn} = (a^n)^k \equiv 1 \pmod{p}$ ist, sobald $a^n \equiv 1 \pmod{p}$ ist, liegt auf der Hand.

Hat man umgekehrt $a^s \equiv 1 \pmod{p}$, so denken wir uns s durch den Exponenten n, zu welchem a gehört, dividirt. Wird der Rest dieser Division r, der Quotient k genannt, so ist $s = kn + r$, also

$$a^s = a^{kn+r} = a^{kn} \cdot a^r .$$

Nun soll $a^s \equiv 1$ sein; a^{kn} ist $\equiv 1$; folglich muss auch

$$a^r \equiv 1 \pmod{p}$$

sein. Da a zum Exponenten n gehört und $r < n$ ist, so ist die letzte Congruenz nur möglich, wenn $r = 0$, also $s = kn$, d. h. ein Vielfaches von n ist.

Lehrsatz III. Wenn der Exponent s einer Potenz von a, durch n dividirt, den Rest r giebt, so ist

$$a^s \equiv a^r \pmod{p} .$$

Beweis. Es sei $s = kn + r$, so ist $a^s = a^{kn} \cdot a^r$, und da $a^{kn} \equiv 1$ ist, so muss $a^s \equiv a^r \pmod{p}$ sein.

Anwendung dieses Satzes. — Um zu bestimmen, welchen Rest 5^{1000} bei der Division durch 7 lässt, sehen wir, zu welchem Exponenten 5 für den Modul 7 gehört. Es ergiebt sich 6. Da nun $1000 = 6 \cdot 166 + 4$ ist, so ist

$$5^{1000} = 5^{6 \cdot 166} \cdot 5^4 \equiv 5^4 \equiv 2 \pmod{7} .$$

§ 47. Vertheilung der Zahlen 1, 2, 3, ..., $(p-1)$ unter die verschiedenen Divisoren von $p-1$ als Exponenten, zu welchen sie für den Modul p gehören. — Wenn eine Zahl a zum Exponenten n gehört und $a^s \equiv 1 \pmod{p}$ ist, so ist, wie wir gesehen haben, n ein Divisor von s. Nun ist aber nach dem Fermat'schen Satze jederzeit $a^{p-1} \equiv 1 \pmod{p}$;

folglich muss der Exponent n, zu welchem eine Zahl a für den Modul p gehört, ein Divisor von $p - 1$ sein.

Es fragt sich jetzt, wie sich die Zahlen 1, 2, 3, ..., $(p - 1)$ unter die verschiedenen Divisoren von $p - 1$ vertheilen, insbesondere ob und wie viele Zahlen zu jedem Divisor als Exponenten gehören. Auf die Zahlen bis $p - 1$ können wir uns deshalb beschränken, weil congruente Zahlen zu demselben Exponenten gehören. Ehe wir die Frage allgemein behandeln, wollen wir sie durch ein Beispiel erläutern.

Es sei $p = 43$; dann hat $p - 1 = 42$ die 8 Divisoren 1, 2, 3, 6, 7, 14, 21, 42, und wir erhalten leicht die Tabelle

Zum Exponenten	gehören die Zahlen
1	1.
2	42.
3	6, 36.
6	7, 37.
7	4, 11, 16, 21, 35, 41.
14	2, 8, 22, 27, 32, 39.
21	9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40.
42	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

Lehrsatz. Zu jedem Divisor d von $p - 1$ gehören als Exponenten genau $\varphi(d)$ Zahlen, wenn durch $\varphi(d)$ ausgedrückt wird, wie viele Zahlen prim zu d und nicht grösser als d sind.

Beweis. Wir nehmen an, es gebe eine Zahl α, die zum Exponenten d gehört, d. h. es sei α^d, aber keine niedrigere Potenz von α der Einheit für den Modul p congruent. Dann muss auch die d^{te} Potenz jeder der d Grössen

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^d$$

$\equiv 1 \pmod{p}$, d. h. eine Wurzel der Congruenz $x^d \equiv 1 \pmod{p}$ sein, und da letztere nicht mehr als d Wurzeln haben kann, so sind die angegebenen Grössen ihre sämmtlichen Wurzeln. Jede zum Exponenten d gehörende Zahl muss sich also unter den Grössen α, α^2, α^3, ..., α^d vorfinden. Wir wollen nun zeigen, dass von diesen Potenzen diejenigen, deren Exponenten prim zu d sind, wirklich zum Exponenten d gehören, die

übrigen aber zu einem niedrigeren Exponenten. Es sei zunächst k prim zu d, so lässt sich eine Zahl m bestimmen, welche der Congruenz $km \equiv 1 \pmod{d}$ genügt. Für diesen Werth von m ist dann $\alpha^{km} \equiv \alpha \pmod{p}$. Gehörte nun die Potenz α^k zu einem Exponenten $e < d$, d. h. wäre $(\alpha^k)^e \equiv 1 \pmod{p}$, so würde auch $\alpha^{mke} \equiv 1 \pmod{p}$ und, da $\alpha^{mk} \equiv \alpha \pmod{p}$ ist, auch $\alpha^e \equiv 1 \pmod{p}$ sein, was der Annahme, α gehöre zum Exponenten d, widerspricht. In diesem Falle gehört also α^k zum Exponenten d.

Wenn dagegen k und d einen grössten gemeinschaftlichen Divisor δ enthalten, so ist schon

$$\left(\alpha^{\frac{k}{\delta}}\right)^d, \text{ also auch } \left(\alpha^k\right)^{\frac{d}{\delta}} \equiv 1 \pmod{p},$$

d. h. α^k gehört zum Exponenten $\frac{d}{\delta}$.

Wenn es demnach überhaupt eine Zahl α giebt, die zum Exponenten d gehört, so gehört auch jede der Potenzen

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^d,$$

deren Exponent prim zu d ist, und solcher giebt es $\varphi(d)$, zu demselben Exponenten. Wir wollen der Kürze halber die Anzahl der Zahlen, die zum Exponenten d gehören, mit $\psi(d)$ bezeichnen. Dann ist $\psi(d)$ entweder Null oder gleich $\varphi(d)$.

Werden nun die Divisoren von $p-1$ mit $d_1, d_2, \ldots, d_n$ bezeichnet, so ist, weil die Zahlen $1, 2, 3, \ldots, p-1$ sämmtlich unter die Divisoren von $p-1$ vertheilt sind,

$$\psi(d_1) + \psi(d_2) + \cdots + \psi(d_n) = p - 1.$$

Nach § 10, Lehrsatz II ist aber auch

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_n) = p - 1,$$

folglich

$$\psi(d_1) + \cdots + \psi(d_n) = \varphi(d_1) + \cdots + \varphi(d_n).$$

Nun ist, wie wir bewiesen haben, jedes Glied der linken Seite entweder gleich Null oder gleich dem entsprechenden Gliede der rechten Seite. Wäre also auch nur ein einziges Glied der linken Seite gleich Null, so könnte die Summe der Glieder der linken Seite nicht gleich derjenigen der rechten sein. Es ist somit für jeden Divisor d

$$\psi(d) = \varphi(d),$$

und das wollten wir beweisen.

§ 48. Primitive Wurzeln. — Nach dem vorhergehenden Satze enthält die Reihe

$$(1) \qquad 1, 2, 3, \ldots, p-1$$

$\varphi(p-1)$ Zahlen, welche zum Exponenten $p-1$ gehören, d. h. von denen die $(p-1)^{te}$, aber keine niedrigere Potenz für den Modul p der Einheit congruent ist. Jede dieser $\varphi(p-1)$ Zahlen wird eine primitive Wurzel von p genannt.

Bezeichnet g eine solche primitive Wurzel von p, so sind die Reste der $p-1$ Potenzen

$$(2) \qquad 1, g, g^2, \ldots, g^{p-2}$$

sämmtlich von einander und von Null verschieden; sie müssen daher in irgend einer Reihenfolge mit den Zahlen (1) übereinstimmen. Wir sind somit im Stande, jede der Zahlen (1) und folglich auch jede durch p nicht theilbare ganze Zahl durch eine ihr congruente Potenz der primitiven Wurzel g zu ersetzen.

So ist z. B. nach der Tabelle in § 44 die Zahl 2 eine primitive Wurzel von 13 und

$$1 \equiv 2^0,\ 2 \equiv 2^1,\ 3 \equiv 2^4,\ 4 \equiv 2^2,$$
$$5 \equiv 2^9,\ 6 \equiv 2^5,\ 7 \equiv 2^{11},\ 8 \equiv 2^3,$$
$$9 \equiv 2^8,\ 10 \equiv 2^{10},\ 11 \equiv 2^7,$$
$$12 \equiv 2^6 \pmod{13}.$$

Kennt man eine primitive Wurzel von p, so ist es leicht, alle übrigen anzugeben. Wir haben nämlich oben bewiesen, dass, wenn a zum Exponenten d gehört, auch die Potenz a^k zu diesem Exponenten gehört, wenn k prim zu d ist. Danach ist jede Potenz g^k einer primitiven Wurzel g von p gleichfalls eine primitive Wurzel von p, wofern k prim zu $p-1$ ist.

Prim zu 12 sind z. B. ausser 1 die Zahlen 5, 7, 11; somit sind ausser 2 auch

$$2^5 \equiv 6,\ 2^7 \equiv 11,\ 2^{11} \equiv 7 \pmod{13}$$

primitive Wurzeln von 13.

§ 49. Berechnung der primitiven Wurzeln. — Lehrsatz. Wenn m und n relative Primzahlen sind und

die Zahl a zum Exponenten m, die Zahl b zum Exponenten n gehört, so gehört das Produkt ab zum Exponenten mn.

Beweis. Da nach unserer Voraussetzung

$$a^m \equiv 1\,,\; b^n \equiv 1 \pmod{p}$$

ist, so ist auch $a^{mn} \equiv 1$, $b^{mn} \equiv 1$, also jedenfalls

$$(ab)^{mn} \equiv 1 \pmod{p}\,.$$

Wir haben daher nur zu zeigen, dass der Exponent, zu welchem ab gehört, nicht kleiner als mn sein kann.

Wird dieser Exponent mit k bezeichnet, ist also

$$(ab)^k \equiv 1 \pmod{p}\,,$$

so wird auch $(ab)^{mk} \equiv 1$, d. h. $a^{mk} \cdot b^{mk} \equiv 1 \pmod{p}$ sein, oder, weil $a^{mk} \equiv 1$ ist, $b^{mk} \equiv 1 \pmod{p}$. Nun gehört aber b zum Exponenten n; folglich muss nach dem Früheren mk durch n, oder, da m prim zu n ist, k durch n theilbar sein.

Ebenso zeigt man, dass k durch m theilbar sein muss. k ist somit durch das Produkt mn theilbar, also jedenfalls nicht kleiner als dieses Produkt.

Mit Hülfe dieses Satzes lässt sich, wie wir jetzt zeigen wollen, für jede Primzahl p ziemlich leicht eine primitive Wurzel ermitteln. Zu diesem Zwecke wählen wir eine beliebige durch p nicht theilbare Zahl a (etwa 2) und schreiben die Reste ihrer Potenzen hin, bis wir zum Rest 1 gelangen. Ist 1 der Rest der k^{ten} Potenz, so gehört a zum Exponenten k. Wenn nun $k = p - 1$ ist, so ist a eine primitive Wurzel von p und die Rechnung beendet. Ist dagegen $k < p - 1$, so wählen wir eine zweite Zahl b, die sich unter den Potenzresten von a nicht vorfindet, und bestimmen durch Berechnung ihrer Potenzreste den Exponenten k', zu welchem sie für den Modul p gehört.

k' kann nun zunächst kein Divisor von k sein; denn sonst wäre $b \equiv a^{\frac{k}{k'}} \pmod{p}$; b würde also der Voraussetzung zuwider einer der Potenzreste von a sein.

Dagegen ist es recht wohl möglich, dass k' ein Vielfaches von k ist. In diesem Falle gehört b zu einem grösseren Exponenten als a, und da wir eine Zahl suchen, die zum

grössten Exponenten, d. i. $p - 1$, gehört, so sind wir unserem Ziele näher gekommen.

Wenn k' kein Vielfaches von k ist, so lässt sich das kleinste gemeinschaftliche Vielfache m von k und k' bestimmen, und dann liefert der oben bewiesene Satz eine Zahl, welche zum Exponenten m gehört. Zerlegt man nämlich m in zwei Factoren k_1, k'_1, die prim zu einander sind und beziehungsweise in k, k' aufgehen, so gehört $a^{\frac{k}{k_1}}$ zum Exponenten k_1, $b^{\frac{k'}{k'_1}}$ zum Exponenten k'_1, folglich $a^{\frac{k}{k_1}} \cdot b^{\frac{k'}{k'_1}}$ zum Exponenten $k' \cdot k'_1 = m$.

Durch wiederholte Anwendung dieses Verfahrens gelangen wir zu Zahlen, die zu immer grösseren Exponenten gehören, also schliefslich einmal zu einer primitiven Wurzel.

Beispiel. Es soll eine primitive Wurzel von 103 bestimmt werden. Die Potenzreste von 2 für den Modul 103 sind

2, 4, 8, 16, 32, 64, 25, 50, 100, 97,
91, 79, 55, 7, 14, 28, 56, 9, 18, 36,
72, 41, 82, 61, 19, 38, 76, 49, 98, 93,
83, 63, 23, 46, 92, 81, 59, 15, 30, 60,
17, 34, 68, 33, 66, 29, 58, 13, 26, 52,
1.

Die Zahl 2 gehört also zum Exponenten 51. Unter den Potenzresten von 2 ist 3 nicht vorhanden. Wir schreiben also auch die Potenzreste dieser Zahl hin

3, 9, 27, 81, 37, 8, 24, 72, 10, 30,
90, 64, 89, 61, 80, 34, 102, 100, 94, 76,
22, 66, 95, 79, 31, 93, 73, 13, 39, 14,
42, 23, 69, 1

und sehen, dass 3 zum Exponenten 34 gehört. Das kleinste gemeinschaftliche Vielfache von $51 = 3 \,.\, 17$ und $34 = 2 \,.\, 17$ ist $102 = 51 \,.\, 2$. Es muss daher $2^{\frac{51}{51}} \,.\, 3^{\frac{34}{2}} = 2 \,.\, 3^{17}$ zum Exponenten 102 gehören, d. h. primitive Wurzel von 103 sein. Da $3^{17} \equiv 102$ ist, so liefert unser Verfahren die primitive Wurzel $2 \,.\, 102 = 204 \equiv 101 \pmod{103}$.

Leichter wären wir in diesem Falle durch folgende Erwägung zum Ziele gelangt: Die Reste von -2 stimmen, ab-

gesehen von den Vorzeichen, mit denen von $+2$ überein. Da nun $2^{51} \equiv 1$ und 51 ungerade ist, so muss $(-2)^{51} \equiv -1$ sein, und somit wird erst die 102te Potenz von -2 den Rest $+1$ liefern. $-2 \equiv 101$ (mod. 103) gehört also zum Exponenten 102 oder ist eine primitive Wurzel von 103.

Wir können nun auch die Potenzreste von 101 ohne Weiteres niederschreiben. Wir schreiben die Reste von 2 zweimal hin, geben dem Rest jeder ungeraden Potenz das Zeichen — und ersetzen jeden negativen Rest durch die ihm congruente kleinste positive Zahl. Wir erhalten auf diese Weise

101, 4, 95, 16, 71, 64 78, 50, 3, 97,
12, 97, 48, 7, 89, 28, 47, 9, 85, 36,
31, 41, 21, 61, 84, 38, 27, 49, 5, 93,
20, 63, 80, 46, 11, 81, 44, 15, 73, 60,
86, 34, 35, 33, 37, 29, 45, 13, 77, 52,
102, 2, 99, 8, 87, 32, 39, 25, 53, 100,
6, 91, 24, 55, 96, 14, 75, 56, 94, 18,
67, 72, 62, 82, 42, 19, 65, 76, 54, 98,
10, 83, 40, 23, 57, 92, 22, 59, 88, 30,
43, 17, 69, 68, 70, 66, 74, 58, 90, 26,
51, 1.

Nun ist jede Potenz von 101, deren Exponent prim zu 102 ist, gleichfalls eine primitive Wurzel von 103. Prim zu 102 sind die 32 Zahlen

1, 5, 7, 11, 13, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 89, 91, 95, 97, 101;

folglich hat 103 die 32 primitiven Wurzeln

101, 71, 78, 12, 48, 85, 21, 84, 5, 20, 11, 44, 86, 35, 45, 77, 99, 87, 53, 6, 96, 75, 67, 62, 65, 54, 40, 88, 43, 70, 74, 51,

von denen 5 die kleinste ist.

§ 50. Die kleinsten primitiven Wurzeln der Primzahlen unter 1000. — Da die Berechnung der primitiven Wurzeln trotz einiger Abkürzungen, die wir übergehen, immerhin ziemlich mühselig ist, so theilen wir für jede ungerade Primzahl unter 1000 die kleinste primitive Wurzel mit und versehen zugleich jede Primzahl, welche die für praktische Rechnungen bequeme primitive Wurzel 10 hat, mit dem Zeichen *.

Primzahl	Prim. Wurzel	Primzahl	Prim. Wurzel	Primzahl	Prim. Wurzel	Primzahl	Prim. Wurzel	Primzahl	Prim. Wurzel	Primzahl	Prim. Wurzel
3	2	113*	3	271	6	443	2	619*	2	821*	2
5	2	127	3	277	5	449	3	631	3	823*	3
7*	3	131*	2	281	3	457	13	641	3	827	2
11	2	137	3	283	3	461*	2	643	11	829	2
13	2	139	2	293	2	463	3	647*	5	839	11
17*	3	149*	2	307	5	467	2	653	2	853	2
19*	2	151	6	311	17	479	13	659*	2	857*	3
23*	5	157	5	313*	10	487*	3	661	2	859	2
29*	2	163	2	317	2	491*	2	673	5	863*	5
31	3	167*	5	331	3	499*	7	677	2	877	2
37	2	173	2	337*	10	503*	5	683	5	881	3
41	6	179*	2	347	2	509*	2	691	3	883	2
43	3	181*	2	349	2	521	3	701*	2	887*	5
47*	5	191	19	353	3	523	2	709*	2	907	2
53	2	193*	5	359	7	541*	2	719	11	911	17
59*	2	197	2	367*	6	547	2	727*	5	919	7
61*	2	199	3	373	2	557	2	733	6	929	3
67	2	211	2	379*	2	563	2	739	3	937*	5
71	7	223*	3	383*	5	569	3	743*	5	941*	2
73	5	227	2	389*	2	571*	3	751	3	947	2
79	3	229*	6	397	5	577*	5	757	2	953*	3
83	2	233*	3	401	3	587	2	761	6	967	5
89	3	239	7	409	21	593*	3	769	11	971*	6
97*	5	241	7	419*	2	599	7	773	2	977*	3
101	2	251	6	421	2	601	7	787	2	983*	5
103	5	257*	3	431	7	607	3	797	2	991	6
107	2	263*	5	433*	5	613	2	809	3	997	7
109*	6	269*	2	439	15	617	3	811*	3		

§ 51. Indices. — Die Bedeutung der primitiven Wurzeln liegt darin, dass sie gestatten, jede durch eine Primzahl p nicht theilbare Zahl durch eine Potenz einer primitiven Wurzel zu ersetzen. Ist nun g eine primitive Wurzel von p, a eine beliebige durch p nicht theilbare Zahl und $a \equiv g^m \pmod{p}$, so nennt man m den Index von a für die Basis g. Da ferner für jede ganze Zahl k $g^{k(p-1)} \equiv 1 \pmod{p}$ ist, so wird auch

$$g^m \cdot g^{k(p-1)}, \text{ d. i. } g^{m+k(p-1)} \equiv a \pmod{p}$$

sein, oder wir können $m + k(p-1)$, d. i. jede Zahl, welche m nach dem Modul $p-1$ congruent ist, als Index von a ansehen und

$$\text{Ind. } a \equiv m \pmod{[p-1]}$$

schreiben. So ist z. B. $101^{20} \equiv 36 \pmod{103}$, also

$$\text{Ind. } 36 \equiv 20 \pmod{102}.$$

Die Indices sind für die Zahlentheorie von grosser Bedeutung. Sie spielen in derselben eine ähnliche Rolle, wie die Logarithmen in der Arithmetik; auch gelten für beide ganz analoge Sätze. Ihr Hauptnutzen beruht auf folgendem Satze:

Lehrsatz. Der Index eines Produkts ist der Summe der Indices der einzelnen Factoren nach dem Modul $p-1$ congruent.

Beweis. Es seien n Zahlen

$$a_1 \equiv g^{m_1},\ a_2 \equiv g^{m_2},\ \ldots,\ a_n \equiv g^{m_n} \pmod{p}$$

gegeben, so dass

$$m_1 \equiv \text{Ind. } a_1,\quad m_2 \equiv \text{Ind. } a_2,\quad \ldots,\quad m_n \equiv \text{Ind. } a_n \pmod{p-1}$$

ist. Durch Multiplication der ersteren Congruenzen erhält man

$$a_1 a_2 \ldots a_n \equiv g^{m_1+m_2+\cdots+m_n} \pmod{p},$$

d. h. es ist

$$\begin{aligned}\text{Ind. } (a_1 a_2 \ldots a_n) &\equiv m_1 + m_2 + \cdots + m_n \\ &\equiv \text{Ind. } a_1 + \text{Ind. } a_2 + \cdots + \text{Ind. } a_n \pmod{p-1}.\end{aligned}$$

Zusatz. Der Index der n^{ten} Potenz einer Zahl ist dem $n$fachen des Index der Zahl nach dem Modul $p-1$ congruent.

Beweis. Wird in der letzten Formel $a_1 = a_2 = \cdots = a_n = a$ angenommen, so geht dieselbe über in

$$\text{Ind. } (a^n) \equiv n \,.\, \text{Ind. } a \pmod{p-1}.$$

Beispiele. Nach der in § 49 gegebenen Tabelle der Potenzreste von 101 für den Modul 103 ist

$$\text{Ind. } 93 \equiv 30,\ \text{Ind. } 3 \equiv 9,\ \text{Ind. } 31 \equiv 21 \pmod{102},$$

also wirklich $\text{Ind. } 93 \equiv \text{Ind. } 3 + \text{Ind. } 31 \pmod{102}$.

Nach derselben Tabelle ist

$$\text{Ind. } 16 \equiv 4,\ \text{Ind. } 2 \equiv 52,$$

also $$\text{Ind. } 16 \equiv 4 \,.\, \text{Ind. } 2 \pmod{102}.$$

§ 52. Auflösung der Congruenz ersten Grades mittels der Indices. — Hat man

$$ax \equiv b \pmod{p},$$

so ist nach dem in § 51 bewiesenen Satze

$$\text{Ind. } a + \text{Ind. } x \equiv \text{Ind. } b \pmod{p-1}$$

oder

$$\text{Ind. } x \equiv \text{Ind. } b - \text{Ind. } a \pmod{p-1}.$$

Wenn man also Tafeln benutzt, welche für jede Zahl den zugehörigen Index und für jeden Index die entsprechende Zahl liefern, so erhält man zunächst den Index von x und sodann den Werth von x selbst. Solche Indextafeln hat Jacobi 1839 für die Primzahlen unter 1000 unter dem Titel „Canon arithmeticus" veröffentlicht. Um ihre Benutzung zu zeigen, lassen wir die beiden Tabellen folgen, die sich auf die Primzahl 43 und die primitive Wurzel 3 beziehen.

I.

Zahl	1	2	3	4	5	6	7	8	9	10	11
Index	42	27	1	12	25	28	35	39	2	10	30
Zahl	12	13	14	15	16	17	18	19	20	21	22
Index	13	32	20	26	24	38	29	19	37	36	15
Zahl	23	24	25	26	27	28	29	30	31	32	33
Index	16	40	8	17	3	5	41	11	34	9	31
Zahl	34	35	36	37	38	39	40	41	42		
Index	23	18	14	7	4	33	22	6	21		

II.

Index	1	2	3	4	5	6	7	8	9	10	11
Zahl	3	9	27	38	28	41	37	25	32	10	30
Index	12	13	14	15	16	17	18	19	20	21	22
Zahl	4	12	36	22	23	26	35	19	14	42	40
Index	23	24	25	26	27	28	29	30	31	32	33
Zahl	34	16	5	15	2	6	18	11	33	13	39
Index	34	35	36	37	38	39	40	41	42		
Zahl	31	7	21	20	17	8	24	29	1		

Beispiel. Die Aufgabe: Ein Gärtner hat weniger als 1000 Bäume. Pflanzt er sie in Reihen von je 53 Stück, so fehlen ihm 10; pflanzt er sie aber in Reihen von je 43 Stück, so bleiben ihm 11 übrig. Wie viel Bäume sind es? führt zu der unbestimmten Gleichung

$$53x - 10 = 43y + 11,$$

welche der Congruenz

$$53x - 10 \equiv 11$$

oder

$$10x \equiv 21 \pmod{43}$$

äquivalent ist. Daraus folgt

$$\text{Ind. } 10 + \text{Ind. } x \equiv \text{Ind. } 21 \pmod{42}$$

oder nach Tabelle I

$$10 + \text{Ind. } x \equiv 36 \pmod{42},$$

$$\text{Ind. } x \equiv 26 \pmod{42}$$

und nach Tabelle II

$$x \equiv 15 \pmod{43}.$$

Es ist also $x = 15 + 43k$, wo k eine unbestimmte Zahl bezeichnet, und man erhält für die Anzahl der Bäume

$$53(15 + 43k) - 10 = 785 + 53 \,.\, 43k.$$

Nun sollen nicht mehr als 1000 Bäume vorhanden sein; folglich muss man $k = 0$ annehmen, so dass sich 785 als die gesuchte Zahl ergiebt.

Anmerkung. — Auf diese Weise lassen sich alle Congruenzen ersten Grades mit einer Unbekannten behandeln, auch diejenigen, welche zusammengesetzte Zahlen zu Moduln haben, da man diese Congruenzen nach § 23 auf solche zurückführen kann, deren Moduln Primzahlen sind.

§ 53. Auflösung der binomischen Congruenz mittels der Indices. — Auch die Congruenzen von der Form

$$(1) \qquad ax^n \equiv b \pmod{p}$$

lassen sich mittels der Index-Tafeln leicht auflösen. Man erhält nämlich aus (1)

$$(2) \qquad n \,.\, \text{Ind. } x \equiv \text{Ind. } b - \text{Ind. } a \pmod{p-1},$$

und somit ist die Auflösung von (1) auf die einer Congruenz ersten Grades mit einer Unbekannten, nämlich Ind. x, zurückgeführt. Für die letztere Congruenz gelten natürlich die in

§ 21 bewiesenen Sätze. Hat man Ind. x bestimmt, so liefern die Indextafeln den Werth, resp. die Werthe von x.

Beispiele. I. Aus $x^7 \equiv 8 \pmod{43}$ folgt

$$7.\,\text{Ind}\,x \equiv 39 \pmod{42} \text{ [Tabelle I]}.$$

Da 42 durch 7 theilbar ist, 39 aber nicht, so ist die letzte Congruenz, folglich auch die vorgelegte nach § 21, Lehrsatz II unmöglich.

II. Aus $x^{11} \equiv 4 \pmod{43}$ folgt

$$11.\,\text{Ind}\,x \equiv 12 \pmod{42} \text{ [Tabelle I]}.$$

Diese Congruenz liefert für die Unbekannte Ind. x den Werth 24, und dann ist nach Tabelle II

$$x \equiv 16 \pmod{43}.$$

III. Liegt die Congruenz

$$x^6 \equiv 11 \pmod{43}$$

vor, so folgt nach Tabelle I

$$6\,\text{Ind}\,x \equiv 30 \pmod{42}$$

oder

$$\text{Ind}\,x \equiv 5 \pmod{7}.$$

Der Index von x hat also (§ 21, Lehrsatz III) die 6 nach dem Modul 42 incongruenten Werthe 5, 12, 19, 26, 33, 40, denen die 6 Werthe von x (Tabelle II)

28, 4, 19, 15, 39, 24

entsprechen.

Am Ende des Werkes sind Indextafeln für die Zahlen unter 100 gegeben. Man löse mittels derselben die Aufgaben:

1) $x^{32} \equiv 20 \pmod{61}$
[9, 23, 38, 52]

2) $x^{17} \equiv 13 \pmod{61}$
[47]

3) $x^4 \equiv 36 \pmod{61}$
[unmöglich]

4) $5x^3 \equiv 7 \pmod{61}$
[7, 24, 30].

§ 54. Uebergang von einem Index-System zu einem andern. — Hat man die Indices der Zahlen

$$1, 2, \ldots, p-1$$

für eine primitive Wurzel g der Primzahl p bestimmt, so ist es leicht, die Indices derselben Zahlen für eine andere primitive Wurzel h derselben Primzahl zu finden.

Es sei

$$a \equiv g^\alpha \quad \text{und} \quad a \equiv h^x \pmod{p},$$

so folgt aus der Congruenz

$$h^x \equiv g^\alpha \pmod{p},$$

wenn allgemein ${}^v\text{Ind.}\, u$ den für die primitive Wurzel v genommenen Index von u bezeichnet,

$$x \equiv \alpha \,.\, {}^h\text{Ind.}\, g \pmod{\overline{p-1}}.$$

Man erhält also den Index einer Zahl für die neue primitive Wurzel h, wenn man den Index α für die frühere primitive Wurzel g mit dem für h genommenen Index von g multiplicirt.

Beispiel. Die Tabelle des § 52 giebt die Indices der Zahlen 1, 2, ... 42 für die primitive Wurzel 3. Um die Indices derselben Zahlen für die primitive Wurzel 5 zu erhalten, hat man ${}^5\text{Ind.}\, 3$, d. i. den Index von 3 für die primitive Wurzel 5 zu ermitteln, also die Congruenz

$$5^x \equiv 3 \pmod{43}$$

zu lösen. Es ergiebt sich der Reihe nach

$$x \,.\, {}^3\text{Ind.}\, 5 \equiv 1 \pmod{42}$$

oder nach Tabelle I

$$25x \equiv 1 \pmod{42}.$$

Diese Congruenz liefert

$$x \equiv 37 \pmod{42}.$$

Wir erhalten somit die Indices der Zahlen 1, 2, ..., 42 für die primitive Wurzel 5, wenn wir die in § 52 angegebenen Werthe mit 37 multipliciren.

§ 55. Zusammenhang zwischen den Indices einer Zahl und dem Exponenten, zu welchem sie gehört. — Da man in Bezug auf jede der $\varphi(p-1)$ primitiven Wurzeln von p den Index einer Zahl a nehmen kann, so hat jede Zahl $\varphi(p-1)$ Indices. So z. B. haben die Zahlen 4, 6, 7, 17, 22 für die verschiedenen primitiven Wurzeln von 43 die in nachstehender Zusammenstellung enthaltenen Indices:

Zahl	gehört zum Exponenten	Index für die primitive Wurzel											
		3	5	12	18	19	20	26	28	29	30	33	34
4	7	12	24	30	12	36	6	18	36	30	24	18	6
6	3	28	28	28	14	28	28	14	14	14	14	28	14
7	6	35	35	35	7	35	35	7	7	7	7	35	7
17	21	38	20	32	10	2	26	22	16	4	34	8	40
22	14	15	9	27	15	3	39	33	3	27	9	33	39.

Die verschiedenen Indices einer und derselben Zahl stehen in einem Zusammenhange mit dem Exponenten, zu welchem die Zahl gehört. Dieser Zusammenhang ist durch die folgenden Sätze ausgedrückt:

Lehrsatz I. Die Zahl $p-1$ und der Index einer Zahl a, derselbe mag genommen sein für welche primitive Wurzel man will, haben den grössten gemeinschaftlichen Divisor $\frac{p-1}{t}$, wenn t den Exponenten bezeichnet, zu welchem a für den Modul p gehört.

Beweis. Da $a^t \equiv 1 \pmod{p}$ ist, so ist t ein Divisor von $p-1$. Ferner ist $g^{\text{Ind.}\,a} \equiv a$, also

$$g^{t \cdot \text{Ind}\,a} \equiv a^t \equiv 1 \pmod{p},$$

also $t\,.\,\text{Ind.}\,a$ ein Vielfaches von $p-1$, oder, da t in $p-1$ aufgeht, Ind. a ein Vielfaches von $\frac{p-1}{t}$, etwa

$$\text{Ind.}\,a = k \cdot \frac{p-1}{t}.$$

Da nun auch $p-1$ ein Vielfaches, nämlich das t-fache, von $\frac{p-1}{t}$ ist, so haben wir nur noch zu zeigen, dass t und k prim zu einander sind.

Hätten beide Zahlen einen grössten gemeinschaftlichen Divisor $d > 1$, wäre etwa

$$k = \varkappa d, \qquad t = \tau d,$$

wo also $\varkappa$, τ als relative Primzahlen vorausgesetzt werden, so würde aus der Congruenz

$$\text{Ind.}\, a \equiv \varkappa d \frac{p-1}{\tau d} \equiv \varkappa \frac{p-1}{\tau} \pmod{p-1}$$

sich

$$a \equiv g^{\varkappa \frac{p-1}{\tau}} \pmod{p}$$

ergeben. Es müsste also

$$a^{\tau} \equiv g^{\varkappa(p-1)} \equiv 1 \pmod{p}$$

sein, d. h. a würde der Voraussetzung zuwider zum Exponenten τ gehören. Es ist also $\frac{p-1}{t}$ der grösste gemeinschaftliche Divisor von $p-1$ und Ind. a.

Lehrsatz II. Jede Zahl a, deren Index, für irgend eine primitive Wurzel genommen, mit $p-1$ den grössten gemeinschaftlichen Divisor d hat, gehört zum Exponenten $\frac{p-1}{d}$.

Beweis. Es sei Ind. $a = d\alpha$ und $p-1 = d\varrho$, wo α und ϱ relative Primzahlen sind. Bezeichnet dann x den Exponenten, zu welchem a gehört, so ist

$$a^x \equiv g^{x \cdot \text{Ind.}\, a} \equiv g^{d\alpha x} \equiv 1 \pmod{p}.$$

Folglich muss $d\alpha x$ durch $p-1 = d\varrho$, oder αx durch ϱ theilbar sein. Nun ist aber α prim zu ϱ; also muss x ein Vielfaches von ϱ sein, und da x die kleinste dieser Bedingung genügende Zahl sein soll, so ist $x = \varrho = \frac{p-1}{d}$.

Anmerkung. — Dieser Satz liefert ein bequemes Mittel, alle Zahlen, die zu irgend einem Divisor d von $p-1$ als Exponenten gehören, ohne Weiteres niederzuschreiben, sobald man die Indices der Zahlen $1, 2, \ldots, p-1$ für eine beliebige primitive Wurzel g bestimmt hat. Man nimmt nämlich alle Indices, die mit $p-1$ den grössten gemeinschaftlichen Divisor $\frac{p-1}{d}$ haben: die zugehörigen Zahlen gehören zum Exponenten d.

Beispiel. Um die Zahlen zu finden, die für den Modul 43 zum Exponenten 7 gehören, nehme man die Indices, welche mit 42 den grössten gemeinschaftlichen Divisor $\frac{42}{7} = 6$ haben. Es sind dies die Indices 6, 12, 18, 24, 30, 36, denen die

Zahlen 41, 4, 35, 16, 11, 21 entsprechen, was mit dem in § 47 erhaltenen Resultat übereinstimmt.

§ 56. Periode der Potenzreste einer Zahl. Summe und Produkt der Glieder. — Bilden wir die Reihe der Potenzreste einer Zahl a für den Modul p, so werden wir, wenn a zum Exponenten t gehört, als t^{ten} Glied 1 erhalten, und von da ab kehren dieselben Reste in derselben Reihenfolge wieder. Die Reste von a bis $a^t \equiv 1$ nennt man die Periode von a, und über diese Periode gelten folgende Sätze:

Lehrsatz I. Die Summe aller Glieder der Periode einer Zahl a ist $\equiv 0 \pmod{p}$.

Beweis. Es sei $1, a, a^2, \ldots, a^{t-1}$ die Periode von a, so ist

$$1 + a + a^2 + \cdots + a^{t-1} = \frac{a^t - 1}{a - 1}.$$

Da nun a zum Exponenten t gehört, also

$$a^t \equiv 1 \pmod{p}$$

ist, so wird diese Summe $\equiv 0 \pmod{p}$ sein, wofern nicht

$$a \equiv 1 \pmod{p}$$

ist. [In diesem Ausnahmefall besteht die Periode aus dem einen Gliede 1].

Beispiele. I. Die Zahl 2 hat für den Modul 17 die Periode 2, 4, 8, 16, 15, 13, 9, 1; die Summe dieser Zahlen ist $68 \equiv 0 \pmod{17}$.

II. Die Zahl 4 hat für den Modul 43 die Periode 4, 16, 21, 41, 35, 11, 1. Die Summe dieser Zahlen ist

$$129 \equiv 0 \pmod{43}.$$

Lehrsatz II. Das Produkt aller Glieder der Periode einer Zahl a ist $\equiv +1$ oder $\equiv -1 \pmod{p}$, jenachdem der Exponent t, zu welchem a gehört, ungerade oder gerade ist.

Beweis. Die Zahl a hat die Periode

$$a, a^2, \ldots, a^t,$$

und das Produkt dieser Zahlen ist

$$P = a^{\frac{1}{2}t(t+1)}.$$

Ist nun erstens $t = 2t' + 1$, also ungerade, so ist

$$P = a^{t(t'+1)}$$

und wegen $a^t \equiv 1$

$$P \equiv 1 \pmod{p}.$$

Wenn dagegen $t = 2t'$, also gerade ist, so ergiebt sich

$$P = a^{t'(2t'+1)} = a^{2t' \cdot t'} \cdot a^{t'} = a^{tt'} \cdot a^{t'}$$

und wegen $a^t \equiv 1$

$$P \equiv a^{t'} \equiv a^{\frac{1}{2}t} \equiv -1 \pmod{p}.$$

Beispiele. I. 2 gehört für den Modul 17 zum Exponenten 8, und die Glieder der Periode von 2 haben das Produkt

$$2 \cdot 4 \cdot 8 \cdot 16 \cdot 15 \cdot 13 \cdot 9 \cdot \equiv 2 \cdot 4 \cdot 8 \cdot (-1)(-2)(-4)(-8)$$
$$\equiv + (2 \cdot 4 \cdot 8)^2 \equiv 64^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}.$$

II. 4 gehört für den Modul 43 zum Exponenten 7, und es ist, da

$$4 \cdot 11 \equiv 1,\ 16 \cdot 35 \equiv 16 \cdot (-8) \equiv -128 \equiv 1$$

und

$$21 \cdot 41 \equiv 21 \cdot (-2) \equiv -42 \equiv 1 \pmod{43}$$

ist, das Produkt der Glieder der Periode

$$4 \cdot 16 \cdot 21 \cdot 41 \cdot 35 \cdot 11 \cdot 1 \equiv 1 \pmod{43}.$$

Anmerkung. — Der letzte Satz liefert einen neuen Beweis des Wilson'schen Satzes. Bezeichnet nämlich a eine primitive Wurzel von p, so enthält die Periode von a alle Zahlen 1, 2, 3, ..., $(p-1)$. Da nun in diesem Falle

$$t = p - 1$$

gerade ist, so muss

$$1 \cdot 2 \cdot 3 \dots (p-1) \equiv -1 \pmod{p}$$

sein.

§ 57. Produkt aller primitiven Wurzeln einer Primzahl. — Die Primzahl 3 hat nur eine primitive Wurzel, nämlich 2. Jede andere ungerade Primzahl hat, wie wir sehen werden, eine gerade Anzahl primitiver Wurzeln, von denen folgender Satz gilt:

Lehrsatz. Das Produkt aller primitiven Wurzeln einer Primzahl p ist $\equiv 1 \pmod{p}$. (Ausgenommen ist der Fall $p = 3$).

Beweis. Bezeichnet g eine primitive Wurzel von p, so

wird g^k alle primitiven Wurzeln dieser Zahl darstellen, wenn man k sämmtliche Werthe annehmen lässt, die prim zu $p-1$ und nicht grösser als $p-1$ sind. Ist aber k ein solcher Werth, so ist es auch $p-1-k$. Für jeden Werth von k, für welchen also g^k eine primitive Wurzel ist, ist auch g^{p-1-k} eine primitive Wurzel, und da

$$g^k \cdot g^{p-1-k} = g^{p-1} \equiv 1 \text{ (mod. } p)$$

ist, so lassen sich die primitiven Wurzeln von p in der Weise in Gruppen von je zweien zusammenstellen, dass das Produkt der beiden Wurzeln jeder Gruppe $\equiv 1$ (mod. p) ist. Es muss also auch das Produkt aller primitiven Wurzeln $\equiv 1$ (mod. p) sein.

Dieser Beweis setzt voraus, dass k, wofern es prim zu $p-1$ ist, auch von $p-1-k$ verschieden sei, und dafs dies in der That der Fall ist, wollen wir jetzt zeigen: Eine ungerade Primzahl kann, durch 4 dividirt, nur 1 oder 3 als Rest geben. Für den Modul 4 zerfallen daher die ungeraden Primzahlen in 2 Klassen, in solche von der Form $4n+1$, wie 5, 13, 17, ... und in solche von der Form $4n+3$, wie 3, 7, 11, ... Wäre nun $k = p-1-k$, so müsste

$$2k = p-1, \qquad k = \frac{p-1}{2}$$

sein. Wenn also p die Form $4n+1$ hätte, so wäre $k = 2n$, und wenn p die Form $4n+3$ hätte, $k = 2n+1$. Die Zahl $k = 2n$ ist aber niemals prim zu $p-1 = 4n$, und

$$k = 2n+1$$

kann nur dann prim zu $p-1 = 4n+2$ sein, wenn $n = 0$, also $p = 3$ ist. Diesen einen Fall ausgenommen, ist also der Satz für alle ungeraden Primzahlen bewiesen.

Beispiel. Für den Modul 43 ist nach § 52

$$3^1 \equiv 3,\ 3^{41} \equiv 29;\quad 3^5 \equiv 28,\ 3^{37} \equiv 20;$$
$$3^{13} \equiv 12,\ 3^{29} \equiv 18;\quad 3^{17} \equiv 26,\ 3^{25} \equiv 5;$$
$$3^{19} \equiv 19,\ 3^{23} \equiv 34;\quad 3^{11} \equiv 30,\ 3^{31} \equiv 33,$$

und wir erhalten

$$3 \cdot 29 = 87 \equiv 1 \text{ (mod. 43)},$$
$$28 \cdot 20 = 560 \equiv 1 \text{ (mod. 43)},$$

$$12 \,.\, 18 = 216 \equiv 1 \pmod{43},$$
$$26 \,.\, 5 = 130 \equiv 1 \pmod{43},$$
$$19 \,.\, 34 = 646 \equiv 1 \pmod{43},$$
$$30 \,.\, 33 = 990 \equiv 1 \pmod{43};$$

also ist auch das Produkt aller primitiven Wurzeln

$$\equiv 1 \pmod{43}.$$

§ 58. Summe der primitiven Wurzeln einer Primzahl. — Der Rest, welchen die Summe aller primitiven Wurzeln einer Primzahl p für den Modul p giebt, kann 0, $+1$ oder -1 sein. Welchen dieser Werthe sie hat, hängt von der Zusammensetzung von $p-1$ ab, wie der folgende Satz von Gauss angiebt:

Lehrsatz. Die Summe aller primitiven Wurzeln einer Primzahl p ist $\equiv 0 \pmod{p}$, wenn $p-1$ durch irgend eine Quadratzahl theilbar ist; sie ist $\pm 1 \pmod{p}$, wenn die Zahl $p-1$ jeden ihrer Primfactoren nur in der ersten Potenz enthält, und zwar ist das obere oder das untere Zeichen zu nehmen, jenachdem die Anzahl dieser ungleichen Primfactoren von $p-1$ gerade oder ungerade ist.

Beispiele. I. 1) 17 hat die 8 primitiven Wurzeln 3, 5, 6, 7, 10, 11, 12, 14, deren Summe $68 \equiv 0 \pmod{17}$ ist.

2) 61 hat die 16 primitiven Wurzeln 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59, deren Summe

$$= 8 \,.\, 61 \equiv 0 \pmod{61}$$

ist. Man beachte, dass 16 selbst eine Quadratzahl, und dass 60 durch 4 theilbar ist.

II. 1) 7 hat die 2 primitiven Wurzeln 3, 5, deren Summe $8 \equiv +1 \pmod{7}$ ist.

2) 11 hat die 4 primitiven Wurzeln 2, 6, 7, 8, deren Summe $23 \equiv +1 \pmod{11}$ ist.

Man beachte, dass $6 = 2 \,.\, 3$, $10 = 2 \,.\, 5$, dass also sowohl 6 wie 10 eine gerade Anzahl Primfactoren enthält.

III. 1) 31 hat die 8 primitiven Wurzeln 3, 11, 12, 13, 17, 21, 22, 24, deren Summe $123 \equiv -1 \pmod{31}$ ist.

2) 43 hat die 12 primitiven Wurzeln 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34, welche die Summe

$$257 \equiv -1 \pmod{43}$$

haben. Es ist $30 = 2 \,.\, 3 \,.\, 5$, $42 = 2 \,.\, 3 \,.\, 7$, also in beiden Fällen die Anzahl der ungleichen Primfactoren von $p - 1$ ungerade.

Beweis. Es sei $p - 1 = a^\alpha b^\beta c^\gamma \ldots$, wo $a, b, c, \ldots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \ldots$ ganze positive Zahlen bezeichnen. Ferner seien

$$A_1, A_2, \ldots, A_{\varphi(a^\alpha)}$$

die $\varphi(a^\alpha)$ Zahlen, welche zum Exponenten a^α gehören,

$$B_1, B_2, \ldots, B_{\varphi(b^\beta)}$$

die $\varphi(b^\beta)$ Zahlen, welche zum Exponenten b^β gehören, u. s. w. Dann ist nach § 49 jedes Produkt $AB \ldots$ eine primitive Wurzel von p (eine zum Exponenten $a^\alpha b^\beta \ldots = p - 1$ gehörende Zahl). Da man nun durch Verbindung jeder der Zahlen A mit jeder der Zahlen B, u. s. w. offenbar

$$\varphi(a^\alpha)\, \varphi(b^\beta) \cdots = \varphi(p-1)$$

Produkte bilden kann, und da p ebenso viele, nämlich $\varphi(p-1)$ primitive Wurzeln besitzt, so wird durch das angegebene Verfahren jede primitive Wurzel und zwar jede nur ein einziges Mal ausgedrückt, wofern jene Produkte für den Modul p incongruent sind.

Dass dies der Fall ist, lässt sich leicht darthun. Wäre nämlich

$$A_m B_n \ldots \equiv A_{m'} B_{n'} \ldots \pmod{p},$$

so würde sich durch Erheben auf die Potenz $b^\beta c^\gamma \ldots$

$$A_m^{b^\beta c^\gamma \ldots} B_n^{b^\beta c^\gamma \ldots} \ldots \equiv A_{m'}^{b^\beta c^\gamma \ldots} B_{n'}^{b^\beta c^\gamma \ldots} \ldots \pmod{p}$$

oder, da

$$B_n^{b^\beta} \equiv B_{n'}^{b^\beta} \equiv \cdots \equiv 1 \pmod{p}$$

sein soll,

$$A_m^{b^\beta c^\gamma \ldots} \equiv A_{m'}^{b^\beta c^\gamma \ldots} \pmod{p},$$

d. h.

$$b^\beta c^\gamma \ldots \operatorname{Ind.} A_m \equiv b^\beta c^\gamma \ldots \operatorname{Ind.} A_{m'} \pmod{a^\alpha b^\beta c^\gamma \ldots},$$

und weiter

$$\operatorname{Ind.} A_m \equiv \operatorname{Ind.} A_{m'} \pmod{a^\alpha}$$

ergeben. Nun ist aber nach § 55 sowohl Ind. A_m, als auch Ind. $A_{m'}$ ein Vielfaches von $b^\beta c^\gamma \ldots$, etwa

$$\text{Ind. } A_m = k b^\beta c^\gamma \ldots, \quad \text{Ind. } A_{m'} = k' b^\beta c^\gamma \ldots.$$

Aus der letzten Congruenz würde somit

$$k \equiv k' \pmod{a^\alpha},$$

also etwa

$$k = k' + \varkappa \cdot a^\alpha$$

folgen. Es wäre demnach, wenn die Basis des Indexsystems mit g bezeichnet wird,

$$A_m = g^{(k' + \varkappa a^\alpha) b^\beta c^\gamma \ldots}, \quad A_{m'} = g^{k' b^\beta c^\gamma \ldots},$$

und weiter

$$A_m = g^{k' b^\beta c^\gamma \ldots} \cdot g^{\varkappa (p-1)} = A_{m'} \cdot g^{\varkappa (p-1)}$$

oder, da $g^{p-1} \equiv 1 \pmod{p}$ ist,

$$A_m \equiv A_{m'} \pmod{p},$$

während doch A_m, $A_{m'}$ incongruent sein sollen.

Die Summe aller primitiven Wurzeln von p ist also identisch mit der Summe aller jener Produkte oder, was dasselbe ist, mit dem Produkt

$$(A_1 + A_2 + \cdots)(B_1 + B_2 + \cdots) \cdots.$$

Suchen wir jetzt einen beliebigen Factor dieses Produkts, etwa

$$A_1 + A_2 + \cdots,$$

d. i. die Summe aller zum Exponenten a^α gehörigen Zahlen zu bestimmen.

Es sei erstens $\alpha = 1$. Ist dann A eine zum Exponenten a gehörende Zahl, so gehören nach § 47 auch die Potenzen $A^2, A^3, \ldots, A^{a-1}$ zu diesem Exponenten, und da nach § 56, I

$$1 + A + A^2 + \cdots + A^{a-1} \equiv 0 \pmod{p}$$

ist, so wird in diesem Falle

$$A + A^2 + \cdots + A^{a-1} \equiv -1 \pmod{p}$$

sein.

Wenn zweitens $\alpha > 1$ und A eine zum Exponenten a^α gehörende Zahl ist, so gehören nach § 47 auch alle diejenigen Potenzen, deren Exponenten prim zu a^α sind, zu diesem Exponenten. Es sind dies die Zahlen

$$A, A^2, A^3, \ldots, A^{a^\alpha - 1}$$

mit Ausschluss der Zahlen

$$A^a,\ A^{2a},\ A^{3a},\ \ldots,\ A^{a^\alpha - a};$$

ihre Summe ist somit

$$(A + A^2 + \cdots + A^{a^\alpha - 1}) - (A^a + A^{2a} + \cdots + A^{a^\alpha - a})$$

oder auch

$$(1 + A + A^2 + \cdots + A^{a^\alpha - 1})$$
$$- (1 + A^a + A^{2a} + \cdots + A^{a^\alpha - a}),$$

und diese Differenz ist $\equiv 0 \pmod{p}$, da nach § 56, I jeder ihrer Theile es ist.

Wir haben oben die Summe aller primitiven Wurzeln von p als ein Produkt

$$(A_1 + A_2 + \cdots)(B_1 + B_2 + \cdots)\cdots$$

von so viel Factoren dargestellt, als $p - 1$ ungleiche Primzahlen $a, b, c, \ldots$ enthält. Wenn nun $p - 1$ eine Primzahl a in einer höheren als der ersten Potenz enthält, so ist der entsprechende Factor $A_1 + A_2 + \cdots$, und somit das ganze Produkt $\equiv 0 \pmod{p}$. Kommt dagegen in der Zahl $p - 1$ jeder ihrer Primzahlfactoren nur in der ersten Potenz vor, so hat jeder Factor jenes Produkts in Beziehung auf den Modul p den Rest -1. Die Summe aller primitiven Wurzeln von p ist also

$$\equiv + 1 \quad \text{oder} \quad \equiv - 1 \pmod{p},$$

jenachdem die Anzahl der ungleichen Primzahlfactoren von $p - 1$ gerade oder ungerade ist.

Anmerkung. — Dieser Satz lässt folgende Verallgemeinerung zu: Die Summe aller zu einem Divisor d von $p - 1$ als Exponenten gehörigen Zahlen ist $\equiv 0 \pmod{p}$, wenn d durch eine Quadratzahl theilbar ist; sie ist $\equiv \pm 1 \pmod{p}$, wenn die Zahl d jeden ihrer Primfactoren nur in der ersten Potenz enthält, und zwar ist das obere oder das untere Zeichen zu nehmen, jenachdem die Anzahl der ungleichen Primfactoren von d gerade oder ungerade ist. Den Beweis, der mit dem vorhergehenden, von einigen Ausdrücken abgesehen, zusammenfällt, übergehen wir. Noch ein Beispiel zur Erläuterung:

Wenn $p = 61$ ist, so hat $p - 1 = 60$ die 12 Divisoren

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60, und es ergiebt sich die folgende Tabelle:

Zum Exponenten	gehören die Zahlen	Summe derselben
2	60	$60 \equiv -1$
3	13, 47	$60 \equiv -1$
4	11, 50	$61 \equiv 0$
5	9, 20, 34, 58	$121 \equiv -1$
6	14, 48	$62 \equiv +1$
10	3, 27, 41, 52	$123 \equiv +1$
12	21, 29, 32, 40	$122 \equiv 0$
15	12, 15, 16, 22, 25, 42, 56, 57	$245 \equiv +1$
20	8, 23, 24, 28, 33, 37, 38, 53	$244 \equiv 0$
30	4, 5, 19, 36, 39, 45, 46, 49	$243 \equiv -1$.
60	Die oben schon angegebenen 16 Zahlen	

Sechstes Kapitel.

Potenzreste für zusammengesetzte Moduln.

§ 59. Periodicität der Reihe der Potenzreste. — **Lehrsatz.** Wenn eine Zahl a prim zum Modul m ist, so befindet sich unter den m ersten Gliedern der Reihe

(1) $$1, a, a^2, \ldots, a^{m-1}, \ldots,$$

abgesehen von der Zahl 1, wenigstens noch ein Glied, welches $\equiv 1 \pmod{m}$ ist.

Beweis. Da a prim zu m ist, so muss auch jedes Glied der Reihe (1) prim zu m sein, d. h. die Reste der Potenzen (1) müssen sich unter den $\varphi(m)$ Zahlen vorfinden, welche prim zu m und nicht grösser als m sind. Da nun in jedem Falle $m > \varphi(m)$ ist, so müssen unter den m ersten Gliedern von (1) zwei Potenzen vorhanden sein, welche denselben Rest haben. Es sei

$$a^{k+n} \equiv a^k \pmod{m}.$$

Da a, also auch a^k prim zu m ist, so kann man diese Congruenz durch a^k dividiren und erhält

$$a^n \equiv 1 \pmod{m},$$

wo $k + n$, also um so mehr $n < m$ ist.

Aus diesem Satze lassen sich dieselben Schlüsse ziehen, wie aus dem entsprechenden Satze für Primzahlmoduln. Wir nennen wieder die kleinste Zahl n, für welche $a^n \equiv 1 \pmod{m}$ ist, den Exponenten, zu welchem die Zahl a für den Modul m gehört. Es bilden dann die Reste der Potenzen

$$1, a, a^2, \ldots, a^{n-1}, a^n, \ldots$$

eine periodische Reihe, indem die Reste der n ersten Glieder (Periode von a), die sämmtlich von einander verschieden sind, sich in unveränderter Folge wiederholen.

So z. B. gehört die Zahl 5 für den Modul 36 zum Exponenten 6; denn es ergiebt sich als Reihe der Potenzreste von 5 für diesen Modul

$$5, 25, 17, 13, 29, 1.$$

§ 60. Der verallgemeinerte Fermat'sche Satz. — Für jede Zahl a, die prim zum Modul m ist, besteht die Congruenz

$$a^{\varphi(m)} \equiv 1 \text{ (mod. } m).$$

Beweis. Es seien

$$(1) \qquad \alpha_1, \alpha_2, \ldots, \alpha_{\varphi(m)}$$

die $\varphi(m)$ Zahlen, welche prim zu m und nicht grösser als m sind. Wird jede dieser Zahlen mit a multiplicirt, so erhalten wir die Produkte

$$(2) \qquad \alpha_1 a, \alpha_2 a, \ldots, \alpha_{\varphi(m)} a,$$

deren Reste von einander verschieden sein müssen; denn aus der Annahme $\alpha_k a \equiv \alpha_\varkappa a$ (mod. m) würde sich durch die hier zulässige Division durch a ergeben, dass $\alpha_k \equiv \alpha_\varkappa$ sein müsste, während α_k und $\alpha_\varkappa$ als von einander verschiedene Zahlen der Reihe (1) vorausgesetzt worden sind. Da nun noch jede der Zahlen (2) prim zu m ist, so müssen die Reste der Produkte (2) in irgend einer Reihenfolge mit den Zahlen (1) übereinstimmen. Es ist daher auch das Produkt aller Zahlen (2) dem Produkte aller Zahlen (1) congruent, also

$$\alpha_1 \alpha_2 \ldots \alpha_{\varphi(m)} a^{\varphi(m)} \equiv \alpha_1 \alpha_2 \ldots \alpha_{\varphi(m)} \text{ (mod. } m),$$

und hieraus folgt durch Division mit $\alpha_1 \alpha_2 \ldots \alpha_{\varphi(m)}$

$$a^{\varphi(m)} \equiv 1 \text{ (mod. } m).$$

Zusatz. Der Exponent, zu welchem eine Zahl a, die prim zum Modul m ist, für diesen Modul gehört, ist ein Divisor von $\varphi(m)$.

Der Beweis stimmt ganz überein mit dem oben für den Satz II des § 46 gegebenen.

§ 61. Vertheilung der Zahlen, die prim zu m sind, unter die Divisoren von $\varphi(m)$ als Exponenten, zu welchen sie für den Modul m gehören. — Beginnen wir der Deutlichkeit halber auch hier mit einigen Beispielen.

Es sei $m = 25$, so hat $\varphi(m) = 20$ die 6 Divisoren 1, 2, 4, 5, 10, 20, und die 20 Zahlen, die prim zu 25 sind, vertheilen sich unter diese Divisoren folgendermafsen:

Zum Exponenten	gehören die Zahlen
1	1
2	24
4	7, 18
5	6, 11, 16, 21
10	4, 9, 14, 19
20	2, 3, 8, 12, 13, 17, 22, 23.

Zweitens sei $m = 15$, so hat $\varphi(m) = 8$ die 4 Divisoren 1, 2, 4, 8, und wir erhalten die Tabelle:

Zum Exponenten	gehören die Zahlen
1	1
2	4, 11, 14
4	2, 7, 8, 13
8	keine.

Drittens sei $m = 98$, so hat $\varphi(m) = 42$ die 8 Divisoren 1, 2, 3, 6, 7, 14, 21, 42, und wir erhalten die Tabelle:

Zum Exponenten	gehören die Zahlen
1	1
2	97
3	67, 79
6	19, 31
7	15, 29, 43, 57, 71, 85
14	13, 27, 41, 55, 69, 83
21	9, 11, 21, 23, 37, 39, 51, 53, 65, 81, 93, 95
42	3, 5, 17, 33, 45, 47, 59, 61, 73, 75, 87, 89.

Endlich sei noch $m = 16$. Dann ist $\varphi(m) = 8$, und wir erhalten die Tabelle:

Zum Exponenten	gehören die Zahlen
1	1
2	7, 9, 15
4	3, 5, 11, 13
8	keine.

Diese Beispiele zeigen, dass der für Primzahlmoduln bewiesene Satz: „Zu jedem Divisor d von $\varphi(p)$ gehören $\varphi(d)$ Zahlen" bei zusammengesetzten Moduln im Allgemeinen nicht gilt. Für die Moduln 15, 16 giebt es keine zu den höchsten Exponenten (in beiden Fällen 8) gehörende Zahl, d. h. 15 und 16 besitzen keine primitiven Wurzeln, während 25 und 98 sich in dieser Beziehung ganz wie Primzahlen verhalten. Da nun die primitiven Wurzeln das Fundament aller weiteren Entwicklungen des vorigen Kapitels waren, so müssen wir zunächst bestimmen, welche zusammengesetzten Zahlen primitive Wurzeln besitzen, und welche nicht.

§ 62. Ermittlung der Zahlen, welche keine primitiven Wurzeln besitzen können. — Jede zusammengesetzte Zahl m lässt sich auf die Form

$$m = 2^{\varkappa} p^{\lambda} q^{\mu} \cdots$$

bringen, wo $\varkappa$, λ, μ, ... ganze positive Zahlen, p, q, ... von einander verschiedene ungerade Primzahlen bezeichnen. Ist nun eine Zahl a prim zu m, so ist sie auch prim zu jedem Factor von m, und wir erhalten nach dem verallgemeinerten Fermat'schen Satze

$$a^{\varphi(2^{\varkappa})} \equiv 1 \pmod{2^{\varkappa}},$$
$$a^{\varphi(p^{\lambda})} \equiv 1 \pmod{p^{\lambda}},$$
$$a^{\varphi(q^{\mu})} \equiv 1 \pmod{q^{\mu}},$$
$$\cdots\cdots\cdots$$

Bezeichnet jetzt M das kleinste gemeinschaftliche Vielfache der Zahlen $\varphi(2^{\varkappa})$, $\varphi(p^{\lambda})$, $\varphi(q^{\mu})$, ..., so ist auch

$$a^{M} \equiv 1 \pmod{2^{\varkappa}},$$
$$a^{M} \equiv 1 \pmod{p^{\lambda}},$$
$$\cdots\cdots\cdots,$$

und da somit die Differenz $a^M - 1$ durch jede der relativen Primzahlen $2^{\varkappa}$, p^{λ}, q^{μ}, ... theilbar ist, so muss sie auch durch das Produkt derselben, d. i. m theilbar sein, d. h. es ist

$$a^{M} \equiv 1 \pmod{m}.$$

Der Exponent, zu welchem a gehört, ist also M oder ein Divisor von M.

Nun wird a eine primitive Wurzel von m sein, wenn es

zum Exponenten $\varphi(m) = \varphi(2^\varkappa)\varphi(p^\lambda)\ldots$ gehört, und dies wird nur dann der Fall sein können, wenn

$$M = \varphi(2^\varkappa)\varphi(p^\lambda)\varphi(q^\mu)\ldots$$

ist, d. h. wenn die Zahlen $\varphi(2^\varkappa)$, $\varphi(p^\lambda)$, ... sämmtlich prim zu einander sind. Offenbar ist aber jede der Zahlen

$$\varphi(p^\lambda) = p^{\lambda-1}(p-1),\ \varphi(q^\mu) = q^{\mu-1}(q-1), \ldots$$

gerade, und ebenso ist $\varphi(2^\varkappa) = 2^{\varkappa-1}$ gerade, wenn $\varkappa > 1$ ist. Daher ist M jedenfalls kleiner als $\varphi(2^\varkappa)\varphi(p^\lambda)\ldots$, oder es giebt keine primitiven Wurzeln in den beiden folgenden Fällen:

1) wenn der Modul m mehr als eine ungerade Primzahl enthält;

2) wenn der Modul m zwar nur eine ungerade Primzahl, aber eine höhere als die erste Potenz von 2 enthält.

Es erübrigt noch, den Fall zu untersuchen, in welchem $m = 2^\varkappa$, also $\varphi(m) = 2^{\varkappa-1}$ ist. Da wir uns überhaupt nur mit den Zahlen beschäftigen, die prim zum Modul sind, so haben wir jetzt nur die ungeraden Zahlen ins Auge zu fassen. Jede solche Zahl a kann, durch 4 dividirt, den Rest 1 oder $3 \equiv -1$ geben, also von der Form

$$a = 1 + 2^2 k \quad \text{oder} \quad a = -1 + 2^2 k$$

sein. Für beide Formen ergiebt sich der Reihe nach

$$\begin{aligned} a^2 &= 1 + 2^3 k_1, \\ a^{2^2} &= 1 + 2^4 k_2, \\ a^{2^3} &= 1 + 2^5 k_3, \\ &\ldots\ldots\ldots, \\ a^{2^{\varkappa-2}} &= 1 + 2^\varkappa k_{\varkappa-2}, \end{aligned}$$

wo $k, k_1, k_2, \ldots, k_{\varkappa-2}$ ganze Zahlen bedeuten. Ist nun $\varkappa > 2$, so liefert die letzte Gleichung

$$a^{\frac{1}{2}\varphi(2^\varkappa)} \equiv 1 \pmod{2^\varkappa};$$

es giebt also drittens keine primitive Wurzel, wenn der Modul eine höhere als die zweite Potenz von 2 ist.

Danach kann es nur in den folgenden drei Fällen primitive Wurzeln geben:

1) wenn der Modul eine Potenz einer ungeraden Primzahl ist;

2) wenn der Modul das Doppelte einer Potenz einer ungeraden Primzahl ist;

3) wenn der Modul gleich 4 ist.

§ 63. Primitive Wurzeln einer Potenz einer ungeraden Primzahl.

Lehrsatz I. Jede primitive Wurzel g von p^λ muss auch primitive Wurzel von p sein.

Beweis. Wir nennen den Exponenten, zu welchem g für den Modul p gehört, x und beweisen, dass $x = p - 1$ sein muss. Da

$$g^x \equiv 1 \pmod{p}$$

sein soll, so können wir

$$g^x = 1 + k_1 p$$

setzen, wo k_1 eine ganze Zahl bezeichnet. Durch Erhebung auf die p^{te} Potenz folgt hieraus

$$g^{xp} = 1 + \frac{p}{1} k_1 p + \frac{p(p-1)}{1 \cdot 2} k_1^2 p^2 + \cdots + k_1^p p^p.$$

Jedes Glied der rechten Seite, mit Ausnahme des ersten Gliedes, ist durch p^2 theilbar. Wir können nun alle diese durch p^2 theilbaren Glieder zusammenfassen und

$$g^{xp} = 1 + k_2 p^2$$

schreiben, wo k_2 eine neue ganze Zahl bezeichnet. Auf diese Weise ergiebt sich weiter

$$\begin{aligned} g^{xp^2} &= 1 + k_3 p^3, \\ g^{xp^3} &= 1 + k_4 p^4, \\ &\cdots\cdots\cdots, \\ g^{xp^{\lambda-1}} &= 1 + k_\lambda p^\lambda, \end{aligned}$$

wo $k_3, \ldots, k_\lambda$ ganze Zahlen bezeichnen. Wegen der letzten Gleichung ist

$$g^{xp^{\lambda-1}} \equiv 1 \pmod{p^\lambda}.$$

Nun soll g eine primitive Wurzel von p^λ sein, also für diesen Modul zum Exponenten $(p-1)p^{\lambda-1}$ gehören. Es muss daher $xp^{\lambda-1}$ ein Vielfaches von $(p-1)p^{\lambda-1}$, d. h. x muss ein Vielfaches von $p - 1$ sein. x ist aber als der Exponent, zu welchem g für den Modul p gehört, auch ein Divisor von $p - 1$. Daher ist $x = p - 1$, d. h. g primitive Wurzel von p.

Lehrsatz II. Eine primitive Wurzel g einer ungeraden Primzahl p ist immer, aber auch nur dann primitive Wurzel von p^λ, wenn die Zahl $g^{p-1}-1$, die nach dem Fermat'schen Satz stets durch p theilbar ist, nicht auch durch p^2 theilbar ist.

Beispiele. 1) Nach § 50 ist 2 primitive Wurzel der Primzahlen 3, 5, 11, 13, 29. Da nun $2^2-1=3$ nicht durch 9, $2^4-1=15$ nicht durch 25, $2^{10}-1=1023$ nicht durch 121, $2^{12}-1=4095$ nicht durch 169 und $2^{28}-1=268435455$ nicht durch 841 theilbar ist, so ist 2 auch primitive Wurzel aller Potenzen 3^m, 5^m, 11^m, 13^m, 29^m, wo m jede ganze positive Zahl sein kann.

2) 3 ist primitive Wurzel von 7 und 17. Nun ist $3^6-1=728$ nicht durch 49 und $3^{16}-1=43046720$ nicht durch 289 theilbar; also ist 3 auch primitive Wurzel aller Potenzen 7^m, 17^m.

Beweis. Bezeichnen wir den Exponenten, zu welchem g für den Modul p^λ gehört, mit x, setzen also

$$(1) \qquad g^x \equiv 1 \pmod{p^\lambda}$$

voraus, so muss nach § 60 x ein Divisor von $\varphi(p^\lambda)=p^{\lambda-1}(p-1)$ sein. Wenn aber die Congruenz (1) besteht, so ist jedenfalls auch

$$(2) \qquad g^x \equiv 1 \pmod{p},$$

also, da g primitive Wurzel von p sein soll, x ein Vielfaches von $p-1$. Daher und weil p prim zu $p-1$ ist, muss x von der Form

$$x = p^y(p-1)$$

sein, wo $y <$ oder $= \lambda - 1$ ist.

Nun ist die Zahl $g^{p-1}-1$ nach dem Fermat'schen Satze jederzeit durch p, möglicherweise aber auch durch eine höhere als die erste Potenz von p theilbar. Es sei p^{1+e} die höchste in $g^{p-1}-1$ aufgehende Potenz von p, also

$$g^{p-1} = 1 + k_1 p^{1+e},$$

so erhalten wir durch Erhebung auf die p^{te} Potenz

$$g^{(p-1)p} = 1 + k_2 p^{e+2},$$
$$g^{(p-1)p^2} = 1 + k_3 p^{e+3},$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad ,$$
$$g^{(p-1)p^y} = 1 + k_{y+1} p^{e+y+1}$$

wo $k_1, k_2, \ldots, k_{y+1}$ ganze Zahlen bedeuten. Daraus folgt, wenn $c + y + 1 = \lambda$ angenommen wird,

$$g^{(p-1)p^{\lambda-1-c}} \equiv 1 \pmod{p^\lambda},$$

d. h. der Exponent, zu welchem g für den Modul p^λ gehört, ist $(p-1)p^{\lambda-1-c}$. Wenn also $c = 0$ ist, so gehört g zum Exponenten $(p-1)p^{\lambda-1} = \varphi(p^\lambda)$; wenn aber c von 0 verschieden ist, so gehört g zu einem Exponenten, der kleiner als $\varphi(p^\lambda)$ ist. Im ersteren Falle ist daher g primitive Wurzel von p^λ, im zweiten Falle nicht.

Lehrsatz III. Die Zahl p^λ besitzt

$$\varphi\varphi(p^\lambda) = \varphi[(p-1)p^{\lambda-1}] = \varphi(p-1)\,\varphi(p^{\lambda-1})$$

primitive Wurzeln.

Beweis. Es sei g eine von den $\varphi(p-1)$ primitiven Wurzeln von p, so wird die Zahl $a = g + kp$, in der k eine ganze Zahl bezeichnet, gleichfalls primitive Wurzel von p sein. a wird nach dem Satz II auch primitive Wurzel von p^λ sein, wenn k so gewählt wird, dass der Ausdruck $a^{p-1} - 1$ nicht durch p^2 theilbar sei. Es ist aber

$$a^{p-1} - 1 = (g + kp)^{p-1} - 1$$
$$= (g^{p-1} - 1) + \frac{p-1}{1} g^{p-2}kp + R,$$

wo R eine Summe von Gliedern bezeichnet, von denen jedes durch p^2 theilbar ist. Damit nun $a^{p-1} - 1$ nicht durch p^2 theilbar sei, darf $\frac{g^{p-1}-1}{p} + (p-1)g^{p-2}k$, welche Zahl wir der Kürze halber A nennen wollen, nicht durch p theilbar sein.

Die Zahl A besteht aus zwei Theilen; der erste Theil $\frac{g^{p-1}-1}{p}$ kann durch p theilbar sein; dann ist A durch p nicht theilbar, wenn der zweite Theil, d. i. $(p-1)g^{p-2}k$ es nicht ist, oder, da $(p-1)$ und g prim zu p sind, wenn k durch p nicht theilbar ist. Ertheilt man also in dem Ausdruck

$$a = g + kp$$

k solche Werthe, die durch p nicht theilbar sind, so stellt derselbe nur primitive Wurzeln von p^λ dar. Will man nur die primitiven Wurzeln erhalten, die für den Modul p^λ incon-

gruent sind, so hat man k die $\varphi(p^{\lambda-1})$ Werthe beizulegen, die prim zu p und nicht grösser als $p^{\lambda-1}$ sind. Auf diese Weise erhält man daher $\varphi(p^{\lambda-1})$ primitive Wurzeln von p^λ.

Wenn der erste Theil von A, d. i. $\frac{g^{p-1}-1}{p}$ nicht durch p theilbar ist, sondern den kleinsten Rest α für p als Modul hat, so ist

$$A \equiv \alpha + (p-1)g^{p-2}k \equiv \alpha - g^{p-2}k \,(\text{mod.}\, p),$$

und da A und

$$Ag \equiv \alpha g - k \,(\text{mod.}\, p)$$

gleichzeitig durch p theilbar sind, so sehen wir, dass A durch p nicht theilbar sein wird, wenn $\alpha g - k$ einen von Null verschiedenen Rest für den Modul p hat, d. h. wenn

$$k = \alpha g + h$$

angenommen wird, wo h jede Zahl sein kann, die prim zu p ist. Für jeden solchen Werth von k stellt der Ausdruck

$$a = g + kp$$

eine primitive Wurzel von p^λ dar. Will man nur die für den Modul p^λ incongruenten primitiven Wurzeln von p^λ nehmen, so darf man h nur die $\varphi(p^{\lambda-1})$ Werthe beilegen, die prim zu p und nicht grösser als $p^{\lambda-1}$ sind. In jedem Falle, A mag durch p theilbar sein oder nicht, liefert also jede primitive Wurzel g von p uns $\varphi(p^{\lambda-1})$ primitive Wurzeln von p^λ.

Dass die primitiven Wurzeln von p^λ, welche aus einer und derselben primitiven Wurzel g von p entstanden sind, von einander verschieden seien, geht aus ihrer Bildungsweise unmittelbar hervor. Es kann aber auch keine der primitiven Wurzeln von p^λ, die einer primitiven Wurzel g von p nach dem Modul p congruent ist, zusammenfallen mit einer primitiven Wurzel von p^λ, die einer zweiten primitiven Wurzel g_1 von p nach dem Modul p congruent ist; denn die Congruenz

$$g + kp \equiv g_1 + k_1 p \,(\text{mod.}\, p^\lambda)$$

würde

$$g + kp \equiv g_1 + k_1 p \,(\text{mod.}\, p)$$

oder

$$g \equiv g_1 \,(\text{mod.}\, p)$$

nach sich ziehen, und dies widerspricht der Voraussetzung,

da g, g_1 als incongruente primitive Wurzeln von p vorausgesetzt werden.

Da nun die Zahl p nach dem Früheren $\varphi(p-1)$ primitive Wurzeln besitzt, da ferner jede derselben $\varphi(p^{\lambda-1})$ primitive Wurzeln von p^λ liefert, die sämmtlich von einander verschieden sind, und da endlich p^λ nach Satz I keine primitive Wurzel besitzt, die nicht auch primitive Wurzel von p (resp. einer primitiven Wurzel von p congruent) wäre, so ersehen wir, dass es für die Zahl p^λ als Modul

$$\varphi(p-1)\,\varphi(p^{\lambda-1}) = \varphi\varphi(p^\lambda)$$

primitive Wurzeln giebt.

§ 64. Ermittlung der primitiven Wurzeln der Potenzen einer ungeraden Primzahl. — Die Schlüsse, welche zum Beweise des vorhergehenden Satzes dienten, liefern uns auch ein Mittel, aus einer primitiven Wurzel g von p die zugehörigen $\varphi(p^{\lambda-1})$ primitiven Wurzeln von p^λ zu berechnen. Wir wollen dies an einem Beispiel zeigen.

Aufgabe. Aus den primitiven Wurzeln 2, 6, 7, 8 von 11 die primitiven Wurzeln von $11^2 = 121$ zu berechnen.

Auflösung. Um zunächst die primitiven Wurzeln von 121 zu finden, welche $\equiv 2 \pmod{11}$ sind, bilden wir den Ausdruck

$$\frac{2^{10}-1}{11} = \frac{1024-1}{11} = 93\,.$$

Da diese Zahl $\equiv 5 \pmod{11}$ ist, so haben wir

$$k = 5\,.\,2 + h$$

zu setzen und h jeden Werth beizulegen, der prim zu 11 ist. Für jeden dieser Werthe wird

$$a = 2 + (10 + h)\,11 = 112 + 11h$$

eine primitive Wurzel von 121. Prim zu 11 und kleiner als 11 sind die 10 Zahlen 1, 2, 3, ..., 10, die wir durch die congruenten Zahlen $-10, -9, \ldots, -1$ ersetzen. Auf diese Weise erhalten wir die 10 primitiven Wurzeln 2, 13, 24, 35, 46, 57, 68, 79, 90, 101.

Zweitens ist wegen

$$\frac{6^{10}-1}{11} = 5496925 \equiv 5 \pmod{11}$$

$$k = 5\,.\,6 + h = 30 + h$$

und

$$a = 6 + (30 + h)\,11 = 336 + 11h$$

zu setzen, und dieser Ausdruck liefert für die incongruenten Werthe von h

$$-30,\ -29,\ -28,\ \ldots\ -23,\ -21,\ -20$$
$$(-22 \text{ muss fehlen})$$

die 10 primitiven Wurzeln

$$6,\ 17,\ 28,\ 39,\ 50,\ 61,\ 72,\ 83,\ 105,\ 116.$$

Drittens ist wegen

$$\frac{7^{10}-1}{11} = 25679568 \equiv 2 \pmod{11}$$
$$k = 2\,.\,7 + h = 14 + h$$

und

$$a = 7 + (14 + h)\,11 = 161 + 11h$$

zu setzen, und man erhält für

$$h = -14,\ -13,\ -12,\ -10,\ -9,\ \ldots,\ -4$$

die 10 primitiven Wurzeln

$$7,\ 18,\ 29,\ 51,\ 62,\ 73,\ 84,\ 95,\ 106,\ 117.$$

Endlich ist wegen

$$\frac{8^{10}-1}{11} = 97612893 \equiv 4 \pmod{11}$$
$$k = 4\,.\,8 + h = 32 + h$$

und

$$a = 8 + (32 + h)\,11 = 360 + 11h$$

zu setzen, und man erhält für

$$h = -32,\ -31,\ -30,\ \ldots,\ -23$$

die 10 primitiven Wurzeln

$$8,\ 19,\ 30,\ 41,\ 52,\ 63,\ 74,\ 85,\ 96,\ 107.$$

§ 65. Primitive Wurzeln des Doppelten einer Potenz einer ungeraden Primzahl. — **Lehrsatz.** Eine ungerade Zahl a gehört für jeden der beiden Moduln p^λ, $2p^\lambda$ zu demselben Exponenten.

Beweis. Wird der Exponent, zu welchem a für p^λ gehört, mit t, derjenige, zu welchem a für $2p^\lambda$ gehört, mit t' bezeichnet, so ist zunächst

$$a^{t'} \equiv 1 \pmod{p^\lambda}.$$

Nun ist aber a, also auch a^t ungerade, d. h.

$$a^t \equiv 1 \pmod{2},$$

und da p^λ prim zu 2 ist, auch

$$a^t \equiv 1 \pmod{2\, p^\lambda}.$$

t muss daher ein Vielfaches von t', d. i. von dem Exponenten sein, zu welchem a für den Modul $2p^\lambda$ gehört.

Aus der Annahme

$$a^{t'} \equiv 1 \pmod{2\, p^\lambda}$$

folgt aber auch

$$a^{t'} \equiv 1 \pmod{p^\lambda},$$

und diese Congruenz lehrt, dass t' ein Vielfaches von t, d. i. von dem Exponenten sein muss, zu welchem a für den Modul p^λ gehört.

Es ist daher $t = t'$, wie zu beweisen war.

Da nun $\varphi(2p^\lambda) = \varphi(2)\,\varphi(p^\lambda) = \varphi(p^\lambda)$ ist, so sehen wir, dass jede ungerade primitive Wurzel von p^λ auch primitive Wurzel von $2p^\lambda$ sein wird. Jede gerade primitive Wurzel von p^λ giebt, wenn wir sie, um sie zu einer ungeraden Zahl zu machen, um p^λ vergrössern, gleichfalls eine primitive Wurzel von $2p^\lambda$, so dafs für den Modul $2p^\lambda$ sich ebenso viele primitive Wurzeln, wie für den Modul p^λ ergeben.

Beispiel. 242 hat mit 121 die 21 ungeraden primitiven Wurzeln 7, 13, 17, 19, 29, 35, 39, 41, 51, 57, 61, 63, 73, 79, 83, 85, 95, 101, 105, 107, 117 gemeinschaftlich. Die 19 geraden primitiven Wurzeln von 121 liefern, wenn jede um 121 vergrössert wird, die 19 letzten primitiven Wurzeln von 242, nämlich 123, 127, 129, 139, 145, 149, 151, 167,
171, 173, 183, 189, 193, 195, 205, 211, 217, 227, 237.

§ 66. Vertheilung der Zahlen, welche prim zum Modul p^λ oder $2p^\lambda$ sind, unter die Divisoren von $\varphi(p^\lambda)$ oder $\varphi(2p^\lambda)$ als Exponenten. — Wir können jetzt die in § 61 angeregte Frage wieder aufnehmen und in aller Strenge beweisen, was sich nach den dort gegebenen Beispielen schon vermuthen liess, dass diejenigen zusammengesetzten Zahlen, welche primitive Wurzeln besitzen, sich auch hinsichtlich der Vertheilung der in Betracht kommenden Zahlen unter die verschiedenen in Betracht kommenden Divisoren als Expo-

nenten genau wie Primzahlen verhalten. Wir können nämlich die folgenden Sätze beweisen:

Lehrsatz I. Jede Potenz g^k einer primitiven Wurzel g von p^λ oder $2p^\lambda$ ist gleichfalls primitive Wurzel dieses Moduls, wofern ihr Exponent k prim zu $p^{\lambda-1}(p-1)$ ist.

Beweis. Wir nehmen an, g^k gehöre für den Modul p^λ oder $2p^\lambda$ zu einem Exponenten t, und beweisen, dass

$$t = p^{\lambda-1}(p-1)$$

sein muss. Da $g^{kt} \equiv 1 \pmod{p^\lambda \text{ oder } 2p^\lambda}$ sein soll, so muss kt ein Vielfaches von $p^{\lambda-1}(p-1)$ sein, also, weil k prim zu $p^{\lambda-1}(p-1)$ ist, t ein Vielfaches dieser Zahl. t soll aber die kleinste Zahl sein, welche den Rest 1 liefert; es ist daher

$$t = p^{\lambda-1}(p-1),$$

d. h. g^k primitive Wurzel von p^λ oder $2p^\lambda$.

Zusatz. Jeder der Moduln p^λ, $2p^\lambda$ besitzt

$$\varphi[p^{\lambda-1}(p-1)] = \varphi\varphi(p^\lambda)$$

primitive Wurzeln.

Lehrsatz II. Jede Potenz g^k einer primitiven Wurzel g, deren Exponent k mit $p^{\lambda-1}(p-1)$ einen grössten gemeinschaftlichen Divisor d hat, gehört zum Exponenten $\frac{p^{\lambda-1}(p-1)}{d}$.

Beweis. Es sei $k = dk'$ und $p^{\lambda-1}(p-1) = dp'$, wo k' und p' relative Primzahlen bezeichnen, so folgt, wenn der Exponent, zu welchem g^k gehört, wieder mit t bezeichnet wird, aus der Congruenz

$$g^{kt} \equiv 1 \pmod{p^\lambda \text{ oder } 2p^\lambda},$$

dass $kt = dk't$ ein Vielfaches von $p^{\lambda-1}(p-1) = dp'$, also $k't$ ein Vielfaches von p' und, da k' prim zu p' ist, t ein Vielfaches von p' sein wird. Da nun t den kleinsten der zulässigen Werthe haben muss, so ist

$$t = p' = \frac{p^{\lambda-1}(p-1)}{d}$$

anzunehmen, d. h. g^k gehört zum Exponenten $\frac{p^{\lambda-1}(p-1)}{d}$.

Anmerkung. Mittels dieses Satzes ist es leicht, sämmtliche Zahlen, die prim zum Modul p^λ oder $2p^\lambda$ sind, unter die

Divisoren von $p^{\lambda-1}(p-1)$ als Exponenten zu vertheilen, sobald man sie als Potenzen einer primitiven Wurzel des Moduls dargestellt hat.

Lehrsatz III. Zu jedem Divisor n von $p^{\lambda-1}(p-1)$ gehören $\varphi(n)$ Zahlen.

Beweis. Zu n als Exponenten gehört jede Potenz g^k einer primitiven Wurzel g, deren Exponent k mit $p^{\lambda-1}(p-1)$ den grössten gemeinschaftlichen Divisor $\frac{p^{\lambda-1}(p-1)}{n} = \alpha$ hat. Alle diese Exponenten k sind Glieder der Reihe

$$\alpha,\ 2\alpha,\ 3\alpha,\ \ldots,\ n\alpha = p^{\lambda-1}(p-1),$$

aus welcher wir, um die Zahlen übrig zu behalten, welche mit $p^{\lambda-1}(p-1)$ keinen Divisor ausser α gemein haben, die Zahlen $m\alpha$ fortzulassen haben, für welche m nicht prim zu $\frac{p^{\lambda-1}(p-1)}{\alpha} = n$ ist. Es bleiben also nur die Glieder $m\alpha$ zurück, bei denen m prim zu n und nicht grösser als n ist, und da die Anzahl dieser Glieder $\varphi(n)$ ist, so gehören zum Divisor n als Exponenten $\varphi(n)$ Zahlen.

§ 67. Auflösung der Congruenz

$$ax^n \equiv b\ (\text{mod. } p^\lambda \text{ oder } 2p^\lambda).$$

Ist g eine primitive Wurzel von p^λ oder $2p^\lambda$, so sind die Reste der Potenzen

$$g,\ g^2,\ g^3,\ \ldots,\ g^{p^{\lambda-1}(p-1)}$$

sämmtlich von einander verschieden, stimmen also in irgend einer Reihenfolge mit den Zahlen überein, welche prim zum Modul und nicht grösser als derselbe sind. Jede dieser Zahlen kann daher durch eine Potenz von g ersetzt werden, und den Exponenten dieser Potenz nennen wir wieder den Index der Zahl. Wenn also

$$a \equiv g^e\ (\text{mod. } p^\lambda \text{ oder } 2p^\lambda)$$

ist, so schreiben wir

$$\text{Ind. } a \equiv e\ [\text{mod. } p^{\lambda-1}(p-1)].$$

Hat man nun wie für die Primzahlmoduln, so auch für die Moduln p^λ und $2p^\lambda$ Indextafeln berechnet, so ist man im Stande, die binomische Congruenz

$$ax^n \equiv b\ (\text{mod. } p^\lambda \text{ oder } 2p^\lambda)$$

mit Leichtigkeit aufzulösen. Man erhält zunächst

$$\text{Ind.}\, a + n\, \text{Ind.}\, x \equiv \text{Ind.}\, b \pmod{p^{\lambda-1}[p-1]};$$

diese Congruenz bestimmt Ind. x, und es liefern sodann die Tafeln den Werth, resp. die Werthe von x.

Beispiel. Es sei die Congruenz

$$3x^7 \equiv 8 \pmod{25}$$

zu lösen. Man erhält

$$\text{Ind.}\, 3 + 7\, \text{Ind.}\, x \equiv \text{Ind.}\, 8 \pmod{20},$$

d. h. nach Tabelle I des Anhangs

$$7 + 7\, \text{Ind.}\, x \equiv 3 \pmod{20},$$

$$7\, \text{Ind.}\, x \equiv -4 \pmod{20}.$$

Diese Congruenz ersten Grades hat die Wurzel

$$\text{Ind.}\, x \equiv 8 \pmod{20},$$

und dann ist nach Tabelle II des Anhangs

$$x \equiv 6 \pmod{25}.$$

Aufgaben. (Die Antworten daneben eingeklammert.)

1. $3x^6 \equiv 47 \pmod{50}$ [$\pm$ 7]
2. $7x^4 \equiv 1 \pmod{9}$ [$\pm$ 4]
3. $4x^2 \equiv 1 \pmod{27}$ [$\pm$ 13]
4. $11x^4 \equiv 9 \pmod{98}$ [$\pm$ 3]
5. $5x^3 \equiv 19 \pmod{98}$ [9; 15; 25]
6. $3x^3 \equiv 17 \pmod{22}$ [7]
7. $7x^7 \equiv 9 \pmod{10}$ [3]
8. $3x^4 + 1 \equiv 0 \pmod{14}$ [$\pm$ 5].
9. Welche Zahlen endigen, auf's Quadrat erhoben, im Siebener System auf 11?

$$x^2 \equiv 8 \pmod{49} \quad [\pm 20].$$

Also die Zahlen $\pm 20 + 49k$, wo k jede ganze Zahl sein kann.

10. $7x^{10} \equiv 29 \pmod{121}$ [$\pm$ 2, $\pm$ 6, $\pm$ 18, $\pm$ 41, $\pm$ 54]
11. $(x-5)^3 \equiv (x+5)^3 \pmod{19}$ [$\pm$ 13]
12. $49x^7 \equiv 3 \pmod{94}$ [3]
13. $5x^3 \equiv 41 \pmod{54}$ [7; 25; 43].

§ 68. Der Modul $2^\varkappa$. — Für den Modul $2^2 = 4$ ist 3 eine primitive Wurzel. Für den Modul $2^\varkappa$, in welchem $\varkappa > 2$ ist, giebt es aber, wie wir in § 62 gesehen haben, keine zum Exponenten $\varphi(2^\varkappa) = 2^{\varkappa-1}$ gehörende Zahl, d. h. keine primitive Wurzel, da, wenn a eine beliebige ungerade Zahl bezeichnet, schon die Potenz $a^{2^{\varkappa-2}} \equiv 1 \pmod{2^\varkappa}$ ist. Die Zahlen, welche prim zum Modul $2^\varkappa$ sind, d. h. die ungeraden Zahlen

$$(1) \qquad 1, 3, 5, \ldots, 2^\varkappa - 1$$

vertheilen sich also unter die Exponenten

$$(2) \qquad 1, 2, 2^2, \ldots, 2^{\varkappa-2},$$

und wir wollen jetzt sehen, wie diese Vertheilung erfolgt.

Zum Exponenten 1 gehört nur die Zahl 1. Jede andere Zahl der Reihe (1) kann durch die Formel

$$a = 2^{n+2}\, k \pm 1$$

ausgedrückt werden, wo $n > 0$ und k ungerade ist. Soll nun a zum Exponenten 2 gehören, so muss

$$a^2 \equiv 1 \pmod{2^\varkappa}$$

sein. Es ist aber

$$a^2 = 2^{n+3}\, k_1 + 1,$$

wo k_1 eine ungerade Zahl bezeichnet, und damit a^2, durch $2^\varkappa$ dividirt, den Rest 1 gebe, muss $n + 3 > \varkappa$ sein. Ist erstens $n + 3 = \varkappa$, also $n + 2 = \varkappa - 1$, so haben wir, damit die Zahl $a = 2^{\varkappa-1}\, k \pm 1$ kleiner als $2^\varkappa$ sei, $k = 1$ anzunehmen. Es gehören also zunächst die beiden Zahlen $2^{\varkappa-1} + 1$, $2^{\varkappa-1} - 1$ zum Exponenten 2. Ist zweitens

$$n + 3 > \varkappa, \quad \text{also} \quad n + 2 > \varkappa - 1,$$

so muss man, da $a < 2^\varkappa$ sein soll, $n + 2 = \varkappa$ und $k = 1$ annehmen, auch das Zeichen $\pm$ durch $-$ ersetzen. Auf diese Weise erhalten wir eine dritte zum Exponenten 2 gehörende Zahl, nämlich $2^\varkappa - 1$. Es gehören also für den Modul $2^\varkappa$ zum Exponenten 2 die drei Zahlen

$$2^{\varkappa-1} - 1, \quad 2^{\varkappa-1} + 1, \quad 2^\varkappa - 1.$$

Um weiter allgemein die Zahlen zu bestimmen, die zum Exponenten 2^t, wo $t > 1$ sein soll, gehören, bilden wir aus

$$a = 2^{n+2}\, k \pm 1$$

die Reihe der Gleichungen

$$a^2 = 2^{n+3}\ k_1 + 1\,,$$
$$a^{2^2} = 2^{n+4}\ k_2 + 1\,,$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\,,$$
$$a^{2^t} = 2^{n+2+t}\,k_t + 1\,,$$

in denen k, k_1, k_2, ..., k_t ungerade Zahlen bezeichnen. Soll nun a für den Modul $2^\varkappa$ zum Exponenten 2^t gehören, so muss wegen der letzten Formel

$$n + 2 + t > \varkappa$$

sein, also

$$n + 2 > \varkappa - t\,.$$

Wäre aber $n + 2 > \varkappa - t$, etwa $n + 2 = \varkappa - t + u$, so würde

$$a^{2^{t-u}} = 2^{n+2+t-u}\,k_{t-u} + 1 = 2^\varkappa\,k_{t-u} + 1$$

sein, d. h. schon die $(2^{t-u})^{\text{te}}$ Potenz von a würde für den Modul $2^\varkappa$ den Rest 1 liefern. Es ist daher $n + 2 = \varkappa - t$ anzunehmen, d. h. zum Exponenten 2^t gehören für den Modul $2^\varkappa$ alle Zahlen von der Form $2^{\varkappa-t}k \pm 1$, wo k solche ungeraden Werthe beizulegen sind, dass die resultirenden Zahlen unter $2^\varkappa$ liegen. Diese Werthe von k sind offenbar

$$1,\ 3,\ 5,\ \ldots,\ 2^t - 1\,.$$

Zu dem Exponenten 2^t gehören also die 2^t Zahlen

$$2^{\varkappa-t} \pm 1,\ 2^{\varkappa-t}\,.\,3 \pm 1,\ 2^{\varkappa-t}\,.\,5 \pm 1,\ \ldots,\ 2^{\varkappa-t}\,.\,(2^t - 1) \pm 1\,.$$

Beispiel. Für den Modul $2^5 = 32$ ergiebt sich sofort die Tabelle

Zum Exponenten	gehören die Zahlen
1	1
2	15, 17, 31
4	7, 9, 23, 25
8	3, 5, 11, 13, 19, 21, 27, 29.

Von besonderem Interesse sind die Zahlen, die zum höchsten in Betracht kommenden Exponenten, zu $2^{\varkappa-2}$ gehören. Wenn der Modul $2^\varkappa = 8$ ist, so gehören die Zahlen 3, 5, 7 zum Exponenten $2^{\varkappa-2} = 2$.

Ist $\varkappa > 3$, so gehören nach dem Früheren zum Exponenten $2^{\varkappa-2}$ die Zahlen

$$2^2+1,\quad 2^2.3+1,\quad 2^2.5+1,\ \ldots,\quad 2^2(2^{\varkappa-2}-1)+1,$$

also alle Werthe, welche der Ausdruck

$$a = 4k + 1$$

annimmt, wenn man k die Werthe $1, 3, 5, \ldots, 2^{\varkappa-2}-1$ beilegt. Wird $k = 2k' + 1$ gesetzt, so wird

$$a = 4(2k'+1) + 1,$$

also entweder

$$8k' + 5 \quad \text{oder} \quad 8k' + 3,$$

und um alle zum Exponenten $2^{\varkappa-2}$ gehörenden Zahlen zu erhalten, haben wir in jeder dieser beiden Formen k' die Werthe $0, 1, 2, \ldots, 2^{\varkappa-3}-1$ zu ertheilen.

Nun zerfallen die unter $2^{\varkappa}$ liegenden $2^{\varkappa-1}$ ungeraden Zahlen nach den Resten, die sie für den Modul 8 liefern, in 4 Klassen von je $\frac{2^{\varkappa-1}}{4} = 2^{\varkappa-3}$ Zahlen, in Zahlen der Formen $8k+1$, $8k+3$, $8k+5$, $8k+7$, und da zum Exponenten $2^{\varkappa-2}$ gerade $2^{\varkappa-3}$ Zahlen jeder der beiden Formen $8k+3$, $8k+5$ gehören, so sehen wir, dass alle Zahlen $8k+3$, $8k+5$ und nur diese zu $2^{\varkappa-2}$ als Exponenten gehören.

Es sei jetzt a eine Zahl von der Form $8k_1+3$, so erhält man leicht die Formeln

$$\begin{aligned} a &= 8k_1+3, \quad & a^2 &= 8k_2+1,\\ a^3 &= 8k_3+3, \quad & a^4 &= 8k_4+1,\\ &\ldots\ldots & &\ldots\ldots\\ a^{2^{\varkappa-2}-1} &= 8k_{2^{\varkappa-2}-1}+3, \quad & a^{2^{\varkappa-2}} &= 8k_{2^{\varkappa-2}}+1, \end{aligned}$$

wo $k_1, k_2, \ldots, k_{2^{\varkappa-2}}$ ganze Zahlen bedeuten. Alle diese Potenzen von a sind, da a zum Exponenten $2^{\varkappa-2}$ gehört, incongruent, und da es zwischen 1 und $2^{\varkappa}$ überhaupt nur je $2^{\varkappa-3}$ Zahlen jeder der Formen $8k+1$, $8k+3$ giebt, so lässt sich jede diesem Intervall angehörende Zahl $8k+1$ oder $8k+3$ als Potenz von a darstellen. Aendert man die Zeichen der Zahlen $8k+1$, $8k+3$ oder nimmt (was dasselbe ist) die Ergänzungen derselben zum Modul, so erhält man auch alle Zahlen $8k+7$, $8k+5$.

Ebenso kann man alle Zahlen der Formen $8k+1$, $8k+5$ als Potenzen der Zahl $a = 8k+5$ darstellen, und die Ergänzungen dieser Zahlen zum Modul sind die Zahlen der Formen $8k+7$, $8k+3$.

Es lässt sich somit jede ungerade Zahl, die kleiner als der Modul $2^\varkappa$ ist, durch eine mit dem Zeichen $+$ oder $-$ genommene Potenz einer Zahl einer der beiden Formen $8k+3$, $8k+5$ ersetzen.

§ 69. Auflösung der binomischen Congruenz

$$ax^n \equiv b \pmod{2^\varkappa}.$$

Gehört die Zahl a für den Modul $2^\varkappa$ zum Exponenten t, so denken wir uns die gegebene Congruenz mit a^{t-1} multiplicirt und erhalten, da $a^t \equiv 1$ ist,

$$x^n \equiv a^{t-1} b \pmod{2^\varkappa}.$$

Wir haben uns also nur mit der Congruenz

$$x^n \equiv a \pmod{2^\varkappa}$$

zu beschäftigen. Um diese aufzulösen, nehmen wir eine zum Exponenten $2^{\varkappa-2}$ gehörende Zahl, am einfachsten 3 oder 5, und schreiben die Reste einer der Reihen

$$3,\ 3^2,\ 3^3,\ \ldots,\ 3^{2^{\varkappa-2}} \tag{1}$$

$$5,\ 5^2,\ 5^3,\ \ldots,\ 5^{2^{\varkappa-2}}, \tag{2}$$

gleichgiltig welcher, hin. Die Reste von (1) geben alle dem in Rede stehenden Intervall angehörigen Zahlen der Formen $8k+1$, $8k+3$ und, mit dem Zeichen $-$ versehen, auch die Zahlen $8k+7$, $8k+5$. Aehnliches gilt von der Reihe (2). Wir können also jede Zahl $8k+1$, $8k+3$, $-(8k+5)$, $-(8k+7)$ durch eine congruente Potenz von 3 ersetzen und den Exponenten dieser Potenz als Index der Zahl (für den Modul $2^{\varkappa-2}$) ansehen und behandeln.

In die Indextafeln sind die Potenzreste von 3 für die Potenzen von 2, soweit diese unter 100 liegen, mit aufgenommen.

Beispiele. 1) $x^2 \equiv 25 \pmod{32}$,

$$2 \operatorname{Ind.} x \equiv 6 \pmod{8},$$

$$\operatorname{Ind.} x \equiv 3 \pmod{4},$$

$$\text{Ind.}\, x \equiv 3,\ 7 \pmod{8},$$
$$x \equiv \pm 5,\ \pm 11 \pmod{32}.$$

2) Die Congruenz $x^7 \equiv 5 \pmod{32}$ ersetzen wir zunächst durch

$$-x^7 \equiv -5 \pmod{32},$$

d. i.

$$(-x)^7 \equiv 27 \pmod{32},$$

und erhalten der Reihe nach

$$7\, \text{Ind.}\, (-x) \equiv 3 \pmod{8},$$
$$\text{Ind.}\, (-x) \equiv 5 \pmod{8},$$
$$-x \equiv 19 \equiv -13 \pmod{32},$$
$$x \equiv 13 \pmod{32}.$$

$$3) \quad x^6 \equiv 13 \pmod{64}$$

ist unmöglich.

$$4) \quad 3x^5 \equiv 31 \pmod{64}$$

multipliciren wir mit $3^{15} \equiv 43$ und erhalten, da

$$31\,.\,43 = 1333 \equiv 53 \pmod{64}$$

ist,

$$x^5 \equiv 53 \pmod{64}$$

und weiter der Reihe nach

$$(-x)^5 \equiv 11 \pmod{64},$$
$$5\,.\,\text{Ind.}\, (-x) \equiv 7 \pmod{16},$$
$$\text{Ind.}\, (-x) \equiv 11 \pmod{16},$$
$$-x \equiv 59 \equiv -5 \pmod{64},$$
$$x \equiv 5 \pmod{64}.$$

§ 70. Die binomische Congruenz im Falle eines beliebig zusammengesetzten Moduls. — Wir sind jetzt im Stande, die Congruenz

$$ax^n \equiv b \pmod{m}$$

für einen beliebig zusammengesetzten Modul zu behandeln. Ist

$$m = 2^\varkappa\, p^\lambda\, q^\mu \ldots,$$

wo $p, q, \ldots$ ungerade Primzahlen, $\varkappa, \lambda, \mu, \ldots$ ganze positive Zahlen bezeichnen, so muss der Ausdruck $ax^n - b$, da er durch m theilbar sein soll, durch jede der Grössen $2^\varkappa$, p^λ,

q^μ, ... theilbar sein, d. h. die vorgelegte Congruenz zieht die folgenden nach sich:

$$ax^n \equiv b \pmod{2^\varkappa},$$
$$ax^n \equiv b \pmod{p^\lambda},$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

Wenn eine dieser Congruenzen unmöglich ist, so ist auch die vorgelegte unmöglich. Bezeichnet dagegen x_1 eine Wurzel der ersten, x_2 eine Wurzel der zweiten Congruenz, u. s. w., so wird jede Zahl X, welche den Bedingungen

$$X \equiv x_1 \pmod{2^\varkappa}, \qquad X \equiv x_2 \pmod{p^\lambda}, \ldots$$

genügt, eine Wurzel der vorgelegten Congruenz sein.

Beispiele. 1) Die Congruenz

$$x^3 \equiv 19 \pmod{800}$$

zieht die beiden folgenden nach sich:

(1) $$x^3 \equiv 19 \pmod{32},$$
(2) $$x^3 \equiv 19 \pmod{25},$$

von denen die erste die Wurzel 11, die zweite die Wurzel 14 hat. Wir haben also

$$X \equiv 11 \pmod{32} \quad \text{und} \quad X \equiv 14 \pmod{25},$$

d. h.

$$11 + 32u = 14 + 25v$$

zu setzen und erhalten

$$7u \equiv 3 \pmod{25},$$
$$u \equiv 4 \pmod{25},$$
$$X = 11 + 32(4 + 25z) \equiv 139 \pmod{800}.$$

2) Die Congruenz

$$5x^2 \equiv 101 \pmod{108}$$

zieht die beiden folgenden nach sich:

(1) $$5x^2 \equiv 101 \pmod{4},$$
(2) $$5x^2 \equiv 101 \pmod{27}.$$

Die erstere hat die beiden Wurzeln ± 1, die zweite die beiden Wurzeln ± 2. Durch Verbindung jeder Wurzel der ersten mit jeder Wurzel der zweiten Congruenz ergeben sich demnach vier Wurzeln der vorgelegten Congruenz, nämlich ± 25, ± 29.

3) Welche Zahlen genügen gleichzeitig den beiden Congruenzen:

$$5x^3 \equiv 19 \pmod{32},$$
$$3x^5 \equiv 35 \pmod{61}?$$

Die erste Congruenz, mit $5^7 \equiv 13 \pmod{32}$ multiplicirt, geht über in

$$x^3 \equiv 23 \pmod{32}$$

und hat nur die eine Wurzel $x \equiv 7 \pmod{32}$.

Die zweite Congruenz hat die 5 Wurzeln 2, 7, 18, 40, 55. Beiden Congruenzen gleichzeitig genügen also die Zahlen 7, 551, 711, 1031, 1543 $+ 1952k$.

§ 71. Die Verwandlung gemeiner Brüche in Decimalbrüche (Gauss, Disquisitiones, 312). — Ein Bruch $\frac{m}{n}$, in welchem m prim zu n und $< n$ vorausgesetzt werden darf, lässt sich bekanntlich nur dann in einen endlichen Decimalbruch verwandeln, wenn es eine durch n theilbare Potenz von 10 giebt, wenn also n die Form $2^\alpha . 5^\beta$ hat, wo α, β ganze positive Zahlen sind, von denen jede auch Null sein kann. In jedem andern Falle setzt sich die Reihe der Decimalstellen ins Unendliche fort.

Ist der Nenner n des vorgelegten Bruches gleich $p^\alpha q^\beta \ldots$, wo $p, q, \ldots$ ungleiche Primzahlen, $\alpha, \beta, \ldots$ ganze positive Zahlen bezeichnen, so können wir nach dem Früheren den Bruch in seine Partialbrüche mit beziehungsweise den Nennern $p^\alpha, q^\beta, \ldots$ zerlegen und jeden dieser Partialbrüche in einen Decimalbruch verwandeln. Wir wollen daher von vorn herein voraussetzen, dass der Nenner n eine Primzahl p oder eine Potenz einer Primzahl p^α sei.

Dies vorausgesetzt, sei e der Exponent, zu welchem die Zahl 10 für den Modul p^α gehört, so sind die Reste der Potenzen

$$10,\ 10^2,\ 10^3,\ \ldots,\ 10^{e-1},\ 10^e,$$

für den Modul p^α genommen, sämmtlich von einander verschieden; dasselbe gilt also auch von den Produkten

$$10 . m,\ 10^2 . m,\ 10^3 . m,\ \ldots,\ 10^e . m,$$

und da $10^e \equiv 1 \pmod{p^\alpha}$ ist, so wird

$$10^e \,.\, m \equiv m$$

sein. Es ist also $10^e \,.\, m$ die erste Zahl dieser Reihe, welche bei der Division durch p^α wieder denselben Rest wie m liefert. Bei der Verwandlung von $\frac{m}{p^\alpha}$ in einen Decimalbruch erhält man demnach e Decimalstellen, welche in unveränderter Reihenfolge wiederkehren, und welche man die Periode des Bruches nennt. Die Anzahl der Stellen der Periode eines Bruches ist also gleich dem Exponenten, zu welchem die Zahl 10 für den Nenner p^α als Modul gehört; sie ist somit vom Zähler ganz unabhängig. Da z. B. $10 \equiv 3$ für den Modul 7 zum Exponenten 6 gehört, so besteht die Periode jedes irreducibelen Bruches mit dem Nenner 7 aus 6 Ziffern.

Hat ein Bruch $\frac{m}{n}$ die Periode $a_1 a_2 \ldots a_e$, und ist

$$m' \equiv m \,.\, 10^\beta \pmod{n},$$

also

$$m' = m \,.\, 10^\beta + kn,$$

wo k eine ganze Zahl bezeichnet, so ergiebt sich

$$\frac{m'}{n} = k + \frac{m}{n} \cdot 10^\beta,$$

d. h. die Periode von $\frac{m'}{n}$ ist gleich derjenigen von $\frac{m}{n} \cdot 10^\beta$ oder gleich $a_{\beta+1}\, a_{\beta+2} \ldots a_e\, a_1\, a_2 \ldots a_\beta$. Wir können also, wenn die Periode eines Bruches $\frac{m}{n}$ berechnet ist, sofort die Periode jedes anderen Bruches $\frac{m'}{n}$ niederschreiben, dessen Zähler dem Produkt von m in eine Potenz von 10 nach dem Modul n congruent ist. So hat z. B. $\frac{1}{7}$ die Periode 142857, und da

$$2 \equiv 1 \,.\, 10^2, \quad 3 \equiv 1 \,.\, 10^1, \quad 4 \equiv 1 \,.\, 10^4, \quad 5 \equiv 1 \,.\, 10^5$$

und $6 \equiv 1 \,.\, 10^3 \pmod{7}$

ist, so sind die Perioden von $\frac{2}{7}$, $\frac{3}{7}$, $\frac{4}{7}$, $\frac{5}{7}$, $\frac{6}{7}$ beziehungsweise

285714, 428571, 571428, 714285, 857142.

So oft, wie in diesem Beispiel, 10 eine primitive Wurzel von n ist, lässt sich jede Zahl, die prim zu n ist, als Potenz

von 10 darstellen; folglich kann man in diesem Falle die Periode jedes irreducibelen Bruches $\frac{m}{n}$ aus derjenigen des Stammbruches $\frac{1}{n}$ ohne Rechnung bilden. Ist dagegen 10 keine primitive Wurzel von n, sondern eine zum Exponenten $\mu < \varphi(n)$ gehörende Zahl, wo dann nach dem Früheren μ ein Divisor von $\varphi(n)$, etwa $\varphi(n) = \lambda\mu$ ist, so lassen sich aus der Periode von $\frac{1}{n}$ nur die Perioden der $\mu - 1$ Brüche entnehmen, deren Zähler $m_1, m_2, \ldots, m_{\mu-1}$ den Potenzen $10, 10^2, \ldots, 10^{\mu-1}$ für den Modul n congruent sind. Wir haben dann die Entwicklungen der μ Brüche

$$(1) \qquad \frac{1}{n}, \quad \frac{m_1}{n}, \quad \frac{m_2}{n}, \quad \ldots, \quad \frac{m_{\mu-1}}{n}.$$

Berechnen wir jetzt weiter (durch wirkliche Division) die Periode eines in der Reihe (1) nicht enthaltenen Bruches $\frac{m'}{n}$, so erhalten wir dadurch zugleich die Perioden der $\mu - 1$ Brüche, deren Zähler $m_1', m_2', \ldots, m'_{\mu-1}$ beziehungsweise den Produkten

$$10 \cdot m', \quad 10^2 \cdot m', \quad 10^3 \cdot m', \quad \ldots, \quad 10^{\mu-1} \cdot m'$$

nach dem Modul n congruent sind, also die Entwicklungen der μ Brüche

$$(2) \qquad \frac{m'}{n}, \quad \frac{m_1'}{n}, \quad \frac{m_2'}{n}, \quad \ldots, \quad \frac{m'_{\mu-1}}{n}.$$

In derselben Weise haben wir weiter mit einem Bruche $\frac{m''}{n}$ zu verfahren, der sich weder in (1), noch in (2) vorfindet, und gelangen dadurch zu einer dritten, vierten, u. s. w. Reihe von Brüchen, bis endlich, nachdem wir $\frac{\varphi(n)}{\mu} = \lambda$ solcher Reihen gebildet haben, alle echten irreducibelen Brüche $\frac{m}{n}$ in Decimalbrüche verwandelt sind.

Beispiel. Für den Modul 13 gehört 10 zum Exponenten 6, und da $\frac{12}{6} = 2$ ist, so vertheilen sich die Brüche mit dem Nenner 13 in zwei Reihen. Es ist mod. 13

$$10^1 \equiv 10, \quad 10^2 \equiv 9, \quad 10^3 \equiv 12, \quad 10^4 \equiv 3, \quad 10^5 \equiv 4,$$

folglich enthält die erste Reihe die Brüche

$$(1) \qquad \frac{1}{13}, \quad \frac{3}{13}, \quad \frac{4}{13}, \quad \frac{9}{13}, \quad \frac{10}{13}, \quad \frac{12}{13},$$

und da $\frac{1}{13}$ die Periode 076923 hat, so haben die 5 übrigen Brüche der Reihe (1) beziehungsweise die Perioden

230769, 307692, 692307, 769230, 923076.

In der Reihe (1) kommt der Bruch $\frac{2}{13}$, der die Periode 153846 hat, nicht vor; nun ist mod. 13

$$2 \,.\, 10 \equiv 7, \quad 2 \,.\, 10^2 \equiv 5, \quad 2 \,.\, 10^3 \equiv 11,$$
$$2 \,.\, 10^4 \equiv 6, \quad 2 \,.\, 10^5 \equiv 8;$$

folglich enthält die zweite Reihe die Brüche

$$(2) \qquad \frac{2}{13}, \quad \frac{5}{13}, \quad \frac{6}{13}, \quad \frac{7}{13}, \quad \frac{8}{13}, \quad \frac{11}{13},$$

von denen die fünf letzten beziehungsweise die Perioden

384615, 461538, 538461, 615384, 846153

haben. (S. auch Gauss, Bd. II, p. 412 ff.).

§ 72. Vermischte Aufgaben.

1) Eine Zahl liegt zwischen 100 und 200. Schreibt man sie im Zahlensystem mit der Grundzahl Fünfzehn, so endet sie mit einer Vier; schreibt man sie aber im System mit der Grundzahl Zwölf, so endet sie mit einer Zehn. Welche Zahl ist es?

$$15x + 4 = 12y + 10$$
$$15x \equiv 6 \text{ (mod. 12), u. s. w. [154].}$$

2) Ein mexikanischer Peso wird getheilt in 32 Cuartillas oder auch in 100 Centavos. Wie kann nun ein Mexicaner einem andern einen halben Centavo bezahlen?

$$\frac{25x}{8} - y = \frac{1}{2}, \quad 25x \equiv 4 \text{ (mod. 8), u. s. w.}$$

[Er zahlt 4 Cuartillas und lässt sich 12 Centavos herausgeben].

3) Den Bruch $\frac{1277}{630}$ in Brüche mit den Nennern 2, 5, 7, 9 zu zerlegen $\cdot \left[\frac{1}{2} + \frac{2}{5} + \frac{4}{7} + \frac{5}{9}\right]$.

4) Welche Zahlen endigen sowohl im Fünfzehner-, wie im Zwölfer-System auf 34?

34 im Fünfzehner-System ist 49 im dekad. System
34 „ Zwölfer- „ „ 40 „ „ „ ,
also liegen die beiden Congruenzen vor

$$a \equiv 49 \pmod{225}, \quad a \equiv 40 \pmod{144}.$$

Die erste liefert $a = 49 + 225x$, und bei Einsetzung dieses Werthes geht die zweite über in

$$49 + 225x \equiv 40 \pmod{144}, \text{ u. s. w.}$$

[$1624 + 3600\,k$, wo $k = 0$ oder jede ganze positive Zahl sein kann].

5) Stellt man ein Regiment, das noch keine 3000 Mann beträgt, zu 3, 4, 5 und 7 auf, so bleibt keiner übrig. Würde man es aber zu 9 und 11 Mann aufstellen, so hätte man im ersten Falle 3 Mann zu wenig, im zweiten 3 zu viel. Wie stark ist das Regiment?

[Die beiden Congruenzen

$$420x \equiv -3 \pmod{9}, \quad 420x \equiv 3 \pmod{11}$$

geben für die gesuchte Zahl 2940].

6) Zwei ganze Zahlen zu suchen, deren Produkt ihren doppelten Unterschied um 100 übertrifft.

$$xy - 2(x - y) = 100, \text{ u. s. w.}$$

$$x = -2 + \frac{96}{y-2}.$$

x	1	2	4	6	10	14	22	46	30	94
y	34	26	18	14	10	8	6	4	5	3

7) Zwei ganze positive Zahlen zu finden, deren Differenz ihrem Quotienten gleich ist.

$$x - y = \frac{x}{y}, \text{ u. s. w.}$$

$$x = y + 1 + \frac{1}{y-1}.$$

[4, 2].

8) Zwei ganze Zahlen anzugeben, deren Produkt das 6fache ihrer Summe ist.

$$xy = 6\,(x + y), \text{ u. s. w.}$$

$$x = 6 + \frac{36}{y-6}$$

[7 u. 42, 8 u. 24, 9 u. 18, 10 u. 15, 12 u. 12].

9) In der, augenscheinlich nicht im dekadischen System geschriebenen, Rechnung

$$121m \text{ à } * 2 \text{ Mk.} = 4422 \text{ Mk.}$$

ist da, wo das Zeichen * steht, eine Ziffer verwischt. Wie heisst diese Ziffer? In welchem System ist die Rechnung geschrieben, und wie wird dieselbe im dekadischen Systeme lauten?

Bezeichnet x die Grundzahl des Systems, y die verwischte Ziffer, so erhalten wir

$$(x^2 + 2x + 1)(xy + 2) = 4x^3 + 4x^2 + 2x + 2$$

und daraus leicht

$$y = 4 - \frac{6}{x+1}.$$

Es ist also entweder $x = 2$, $y = 2$ oder $x = 5$, $y = 3$; da aber im Zweier-System eine Ziffer 2 nicht existirt, so ist die erste Lösung zu verwerfen. Die Rechnung ist also im Fünfer-System geschrieben, die verwischte Ziffer ist 3, und die Rechnung lautet im dekadischen System

$$36m \text{ à } 17 \text{ Mk.} = 612 \text{ Mk.}$$

10) In einer Gesellschaft von 30 Personen (Männern und Frauen) verzehrt ein Mann doppelt so viel als eine Frau. Wenn sich nun die Rechnung auf 55,50 Mk. beläuft, wie viel Personen von jeder Art sind dann in der Gesellschaft?

Es seien x Männer, also $30 - x$ Frauen; jeder Mann verzehre $2y$ Pf., jede Frau also y Pf., so erhalten wir die Gleichung

$$2xy + 30y - xy = 5550,$$

und daraus folgt leicht $y = \frac{5550}{x+30}$.

[20 Männer, jeder 2,22 Mk. und 10 Frauen, jede 1,11 Mk.
7 „ „ 3 „ „ 23 „ „ 1,50 „].

11) Welche Reste lässt die Zahl $2^{64} - 1$ bei der Division durch 3, 5, 7, 11, 13, 17, 19?

[0, 0, 1, 4, 2, 0, 16].

11*) Welchen Rest lässt die Potenz 7359^{4431} bei der Division durch 79?

Es ist $7359 \equiv 12 \pmod{79}$, und 12 gehört für den Modul 79 zum Exponenten 26. Da nun $4431 \equiv 11 \pmod{26}$ ist, so ist

$$7359^{4431} \equiv 12^{4431} \equiv 12^{11} \equiv 17 \pmod{79}.$$

12) Jemand hat weniger als 10 Bücherschränke; jeder Schrank hat doppelt so viel Gefächer, als Schränke da sind, und jedes Gefach enthält 10mal so viel Bände, als Gefächer in einem Schranke sind. Bei einem Umzug werden die Bücher in Körbe gelegt, von denen jeder 121 Bände fasst. Dabei stellt sich heraus, dass der letzte Korb nicht voll wird, sondern noch 9 Bände mehr aufnehmen könnte. Wie viel Schränke sind es?

Für die Anzahl x der Schränke ergiebt sich die Congruenz

$$40x^3 \equiv 112 \pmod{121}, \text{ u. s. w.}$$

[3 Schränke à 6 Gefächer à 60 Bde., also 1080 Bände.]

13) Zwei arithmetische Reihen haben gleiche Endglieder. Die erste hat zum Anfangsglied 9 und zur Summe 25, die zweite zum Anfangsgliede 8 und zur Summe 36. Wie viel Glieder hat jede der Reihen?

Wenn die Zahl der Glieder der ersten Reihe mit x, die der zweiten mit y bezeichnet wird, so erhalten wir die beiden Gleichungen

$$\frac{(9+t)x}{2} = 25, \quad \frac{(8+t)y}{2} = 36$$

und durch Elimination des Endgliedes t

$$50y = 72x + xy,$$

woraus sofort

$$x = \frac{50y}{y+72} = 50 - \frac{3600}{y+72}$$

sich ergiebt. Eine Betrachtung der 45 Divisoren von 3600 liefert dann die 21 verschiedenen Lösungen

x	2	5	10	14	20	25	26	30	32	34	35
y	3	8	18	28	48	72	78	108	128	153	168
x	38	40	41	42	44	45	46	47	48	49	
y	228	288	328	378	528	648	828	1128	1728	3528	

14) Zwei arithmetische Reihen haben gleiche Anfangsglieder. Die erste hat zum letzten Gliede 39 und zur Summe aller Glieder 207, die zweite zum letzten Gliede 124 und zur Summe aller Glieder 917. Wie viel Glieder hat jede?

Das Anfangsglied jeder Reihe sei a. Hat dann die erste Reihe x, die zweite y Glieder, so ist

$$\frac{a+39}{2}x = 207\,,\quad \frac{a+124}{2}y = 917\,,$$

und daraus folgt durch Elimination von a

$$414y + 85xy = 1834x\,,$$

$$y = \frac{1834x}{85x + 414}\,,$$

$$85y = \frac{1834x \cdot 85}{85x + 414} = 1834 - \frac{759276}{85x + 414}\,.$$

Die Betrachtung der 72 Divisoren von

$$759276 = 2^2 \cdot 3^2 \cdot 7 \cdot 23 \cdot 131$$

ergiebt nur die eine Lösung $x = 9$, $y = 14$.

(Da der Divisor, um 414 vermindert, durch 85 theilbar sein soll, so sind nur die auf 4 oder 9 endigenden Divisoren ins Auge zu fassen.)

15) Die wievielte Potenz von 7 lässt bei der Division durch 61 den Rest 4?

$$7^x \equiv 4 \pmod{61}\,,$$

$$x \cdot \text{Ind.}\,7 \equiv \text{Ind.}\,4\,,\ \text{d. i.}\ 49x \equiv 2 \pmod{60}\,,\ \text{u. s. w.}\ [38]$$

16[a]) Welche Reste können Potenzen von 4 für den Modul 9 haben, und welche nicht? Bezeichnet m eine beliebige ganze positive Zahl, y den Rest, so soll untersucht werden, für welche Werthe von y die Congruenz

$$4^m \equiv y \pmod{9}$$

möglich ist, und für welche nicht. Wir erhalten

$$2m \equiv \text{Ind.}\,y \pmod{6}\,.$$

Es muss also Ind. y eine gerade Zahl sein, d. h. y kann nur die Werthe 4, 7, 1 haben.

16[b]) Welche Reste können die Potenzen von 5 für den Modul 22 haben, und welche nicht?

[möglich sind nur 1, 3, 5, 9, 15].

17) Für welche Werthe von x und y besteht die Congruenz

$$3^x \equiv y^5 \pmod{61}?$$

Man erhält $6x \equiv 5 \,\text{Ind.}\, y \pmod{60}$, woraus hervorgeht, dass Ind. y durch 6 theilbar sein muss. Hat nun Ind. y einen der Werthe 0, 12, 24, 36, 48, so ergiebt sich $x \equiv 0 \pmod{10}$. Ist dagegen Ind. y eine der Zahlen 6, 18, 30, 42, 54, so wird $x \equiv 5 \pmod{10}$ sein. Daher besteht die Congruenz

$$3^{10k} \equiv y^5 \pmod{61},$$

in welcher $k = 0$ oder eine beliebige ganze positive Zahl ist, nur für die Werthe von y, welche mod. 61 einen der Reste 1, 9, 20, 34, 58 geben, und die Congruenz

$$3^{5+10k} \equiv y^5 \pmod{61}$$

nur für solche y, welche mod. 61 einen der Reste 3, 27, 41, 52, 60 haben.

18) Drei Armee-Corps A, B, C, von denen A aus 5 Regimentern besteht, werden ins Feld geschickt. Mit dem gesammten Proviant würde C eine ganze Anzahl von Wochen auskommen, B 40 Wochen länger als C, A 24 Wochen länger als B. Aus wie viel Regimentern bestehen B und C, und wie lange würde der Vorrath für jedes Corps reichen?

Die 5 Regimenter von A kommen $z + 64$ Wochen aus, die x von B $z + 40$ Wochen, die y von C z Wochen. Es ist also

$$5z + 320 = xz + 40x = yz.$$

Aus $xz + 40x = 5z + 320$ folgt

$$x = \frac{5z + 320}{z + 40} = 5 + \frac{120}{z + 40},$$

und daraus ergeben sich die beiden Lösungen

$$z = 20, \quad x = 7;$$

$$z = 80, \quad x = 6.$$

Für die erstere folgt weiter $y = 21$, für die zweite $y = 9$.

19) Den Bruch $x = \frac{1146185}{306306}$ auf 30 Stellen genau in einen Decimalbruch zu verwandeln, ohne mit dem Nenner in den Zähler zu dividiren.

Durch Zerlegung des gegebenen Bruchs in Partialbrüche erhält man

$$x = \frac{1}{2} + \frac{5}{7} + \frac{7}{9} + \frac{8}{11} + \frac{11}{13} + \frac{3}{17}.$$

Ferner ist

$$\frac{1}{17} = 0{,}058\ 823\ 529\ 411\ 764\ 7 \,|\, 058 \cdots$$

und

$$3 \equiv 10^{11} \pmod{17}.$$

Es ergiebt sich somit

$$\begin{aligned}
\frac{1}{2} &= 0{,}5 \\
\frac{5}{7} &= 0{,}714\ 285\ 714\ 285\ 714\ 285\ 714\ 285\ 714\ 285\ 71 \cdots \\
\frac{7}{9} &= 0{,}777\ 777\ 777\ 777\ 777\ 777\ 777\ 777\ 777\ 777\ 77 \cdots \\
\frac{8}{11} &= 0{,}727\ 272\ 727\ 272\ 727\ 272\ 727\ 272\ 727\ 272\ 72 \cdots \\
\frac{11}{13} &= 0{,}846\ 153\ 846\ 153\ 846\ 153\ 846\ 153\ 846\ 153\ 84 \cdots \\
\frac{3}{17} &= 0{,}176\ 470\ 588\ 235\ 294\ 117\ 647\ 058\ 823\ 529\ 41 \cdots \\
x &= 3{,}741\ 960\ 653\ 725\ 359\ 607\ 712\ 548\ 889\ 019\ \ 5
\end{aligned}$$

20) Ein irreducibeler Bruch hat zum Nenner 256; bei seiner Verwandlung in einen Kettenbruch hat der vorletzte Näherungsbruch den Nenner 35. Welches ist der Bruch?

Wir bezeichnen die Zähler des Bruchs und seines vorletzten Näherungsbruchs beziehungsweise mit x und y; dann ist, wenn e r s t e n s eine gerade Anzahl unvollständiger Quotienten vorhanden ist,

$$35x - 256y = +1,$$

und daraus folgt leicht

$$x = 256k - 117, \quad y = 35k - 16,$$

wo k unbestimmt bleibt. Für $k = 1$ z. B. ergiebt sich als Werth des Bruchs $\frac{139}{256}$.

Wenn aber z w e i t e n s die Anzahl der unvollständigen Quotienten ungerade ist, so ist

$$35x - 256y = -1,$$

und daraus ergiebt sich

$$x = 256k + 117, \quad y = 35k + 16,$$

somit für $k = 1$ als Werth des Bruchs $\frac{373}{256}$.

21) Welche gleichnamigen Brüche sind so beschaffen, dass ihre Differenz gleich der Differenz ihrer Kuben ist?

Werden die Brüche $\frac{m}{n}$ und $\frac{p}{n}$ genannt, so soll

$$\frac{m^3}{n^3} - \frac{p^3}{n^3} = \frac{m}{n} - \frac{p}{n},$$

also

$$\frac{m^2}{n^2} + \frac{mp}{n^2} + \frac{p^2}{n^2} = 1$$

oder

$$(1) \qquad m^2 + mp + p^2 = n^2$$

sein. Wir setzen demgemäss

$$m^2 + mp + p^2 = (m + kp)^2;$$

dann folgt

$$m + p = 2mk + k^2p,$$

also

$$\frac{p}{m} = \frac{1 - 2k}{k^2 - 1}.$$

Weiter ist $n = \pm (m + kp)$, also

$$\frac{n}{m} = \pm\left(1 + k\frac{p}{m}\right) = \pm\left(\frac{-k^2 + k - 1}{k^2 - 1}\right),$$

und die gesuchten Brüche sind

$$\frac{m}{n} = \pm\frac{k^2 - 1}{-k^2 + k - 1}, \quad \frac{p}{n} = \frac{p}{m} : \frac{n}{m} = \pm\frac{1 - 2k}{-k^2 + k - 1}.$$

Für $k = -2$ erhält man z. B. $\pm\frac{3}{7}$, $\pm\frac{5}{7}$, für $k = -3$ ebenso $\pm\frac{8}{13}$, $\pm\frac{7}{13}$; u. s. w.

22) Der Ausdruck $3x^2 + 5x + 8$ wird für $x = 1$ ein Quadrat. Für welche sonstigen rationalen Werthe von x wird derselbe ein Quadrat?

Setzt man $x = 1 + ky$, so geht der gegebene Ausdruck über in $16 + 11\,ky + 3k^2y^2$. Dies soll ein Quadrat werden. Wir setzen also

$$16 + 11\,ky + 3k^2y^2 = (4 + my)^2$$

und erhalten

$$y = \frac{8m - 11k}{3k^2 - m^2},$$

$$x = \frac{8km - 8k^2 - m^2}{3k^2 - m^2} = 1 + \frac{k(8m - 11k)}{3k^2 - m^2},$$

wo k und m unbestimmt sind.

Für $k = 1$, $m = 1$ ist z. B. $x = -\frac{1}{2}$.

23) Es soll gezeigt werden, dass 2620 und 2924 befreundete Zahlen sind.

$$2620 = 2^2 \cdot 5 \cdot 131$$

hat als Summe der Divisoren

$$(1 + 2 + 2^2)(1 + 5)(1 + 131) = 5544,$$

und es ist

$$5544 - 2620 = 2924.$$

$$2924 = 2^2 \cdot 17 \cdot 43$$

hat als Summe der Divisoren

$$(1 + 2 + 2^2)(1 + 17)(1 + 43) = 5544,$$

und es ist

$$5544 - 2924 = 2620.$$

24) Die Gleichung $5x + 7xy + 6y - 13y^2 = 17$ in ganzen Zahlen zu lösen.

Man erhält

$$x = \frac{13y^2 - 6y + 17}{7y + 5}$$

und durch Division

$$49x = 91y - 107 + \frac{1368}{7y + 5}.$$

Von den 24 Divisoren der Zahl $1368 = 2^3 \cdot 3^2 \cdot 19$ haben nur vier, nämlich 12, 19, 152, 684 die Eigenschaft, um 5 vermindert durch 7 theilbar zu werden. Für diese 4 Divisoren ergiebt sich beziehungsweise

$$y_1 = 1, \quad 49x_1 = 98, \quad x_1 = 2$$

$$y_2 = 2, \quad 49x_2 = 147, \quad x_2 = 3$$

$$y_3 = 21, \quad 49x_3 = 1813, \quad x_3 = 37$$

$$y_4 = 97, \quad 49x_4 = 8722, \quad x_4 = 178.$$

25) Desgleichen die Gleichung

$$15x + 7y^2 - 6y = 175.$$

Es ergiebt sich

$$x = 11 + \frac{10 + 6y - 7y^2}{15},$$

und man erhält leicht die 4 Lösungen

$$\begin{aligned}
x_1 &= -14 + 104k - 105k^2, & y_1 &= -7 + 15k \\
x_2 &= -\ \ 2 + \ 76k - 105k^2, & y_2 &= -5 + 15k \\
x_3 &= \quad 9 + \ 35k - 105k^2, & y_3 &= -2 + 15k \\
x_4 &= \quad 2 - \ 64k - 105k^2, & y_4 &= +5 + 15k.
\end{aligned}$$

Die einzigen positiven Werthe von x, y, die der Gleichung genügen, enthält die 4[te] Lösung, die für $k = 0$ $x = 2$, $y = 5$ liefert.

26) Die Zahl 937 in zwei Quadrate zu zerlegen.

Die Congruenz $x^2 + 1 \equiv 0 \pmod{937}$ hat die Wurzeln $x \equiv \pm 196$; der Bruch $\frac{937}{196}$ liefert, in einen Kettenbruch entwickelt, die unvollständigen Quotienten 4, 1, 3, 1, 1, 3, 1, 4. Näherungsbrüche:

	4	1	3	1
$\frac{1}{0}$	$\frac{4}{1}$	$\frac{5}{1}$	$\frac{19}{4}$	$\frac{24}{5}$

Zerlegung: $937 = 19^2 + 24^2$.

27) Die Zahl $\pi = 3{,}14159\,26535\ldots$ in einen Kettenbruch zu verwandeln und die ersten 5 Näherungsbrüche anzugeben.

Unvollständige Quotienten: 3, 7, 15, 1, 292, 1, 1, 37, . .

Näherungsbrüche:

3	7	15	1	. .	. . .
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{22}{7}$	$\frac{333}{106}$	$\frac{355}{113}$	. . .

$$\frac{355}{113} = 3{,}1415929\ldots$$

also auf 6 Stellen genau.

28) Die Seite eines Quadrats verhält sich zum Radius eines Kreises von gleicher Grösse wie $1{,}7724539\ldots : 1$ Dieses Verhältniss soll durch kleinere Zahlen ausgedrückt werden.

Unvollständige Quotienten: 1, 1, 3, 2, 1, 1, 6, 1, 29, . . .

Näherungsbrüche:

1	1	3	2	1	1	6	...	
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{7}{4}$	$\frac{16}{9}$	$\frac{23}{13}$	$\frac{39}{22}$	$\frac{257}{145}$	...

29) Ermittle die Gleichungen, deren Wurzeln die unendlichen periodischen Kettenbrüche

1) $\frac{1}{1+\frac{1}{3+\frac{1}{5+\frac{1}{7+\frac{1}{9+\frac{1}{1+\cdot_{\cdot_{\cdot}}}}}}}}$ 2) $2+\frac{1}{3+\frac{1}{4+\frac{1}{2+\cdot_{\cdot_{\cdot}}}}}$ 3) $3+\frac{1}{2+\frac{1}{2+\cdot_{\cdot_{\cdot}}}}$

sind.

1) Der erste Bruch hat die Näherungsbrüche:

0	1	3	5	7	$9+x$	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{3}{4}$	$\frac{16}{21}$	$\frac{115}{151}$	$\frac{115(9+x)+16}{151(9+x)+21}$,

also ist

$$x = \frac{115(9+x)+16}{151(9+x)+21}.$$

2)

2	3	4	x
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{7}{3}$	$\frac{30}{13}$

$$x = \frac{30x+7}{13x+3}.$$

3) Es ist $x - 3 = \frac{1}{2+(x-3)} = \frac{1}{x-1}$; also

$$(x-3)(x-1) = 1.$$

30) Verwandle $\sqrt{7}$ in einen Kettenbruch.

Unvollständige Quotienten: 2, (1, 1, 1, 4), (1, ...

31) Welche Quadratwurzel liefert den unendlichen periodischen Kettenbruch, dessen unvollständige Quotienten 6, (1, 5, 1, 12), (1, ...) sind?

Es ist $$x - 6 = \frac{1}{1+\frac{1}{5+\frac{1}{1+\frac{1}{12+(x-6)}}}}.$$

Näherungsbrüche:

0	1	5	1	$x+6$	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{5}{6}$	$\frac{6}{7}$	$\frac{6(x+6)+5}{7(x+6)+6}$.

Also ist
$$x - 6 = \frac{6(x+6)+5}{7(x+6)+6},$$
und daraus ergiebt sich
$$x = \sqrt{47}\,.$$

32) Eine Lösung der Gleichung $x^2 - 96y^2 = 1$ zu ermitteln.

Der Kettenbruch, den $\sqrt{96}$ liefert, hat die Reihe der unvollständigen Quotienten
$$9,\ (1,\ 3,\ 1,\ 18),\ (1,\ \ldots$$
Näherungsbrüche:

9	1	3	1	18	...
$\frac{1}{0}$	$\frac{9}{1}$	$\frac{10}{1}$	$\frac{39}{4}$	$\frac{49}{5}$	...

Lösung: $x = 49,\ y = 5\,.$

33) Drei ungleiche Zahlen von der Beschaffenheit zu bestimmen, dass die Summe ihrer Quadrate gleich ist der Summe der Differenzen je zweier dieser Quadrate.

Werden die Zahlen x, y, z genannt, wo $x > y > z$ vorausgesetzt wird, so soll
$$x^2 + y^2 + z^2 = (x^2 - y^2) + (y^2 - z^2) + (x^2 - z^2),$$
d. h.
$$x^2 - y^2 = 3z^2$$
oder
$$(x+y)(x-y) = 3zz$$
sein. Die Annahme $x + y = 3z$, $x - y = z$ würde $y = z$ liefern. Von den übrigen zulässigen Annahmen wählen wir etwa
$$x + y = z^2,\ x - y = 3\,;$$
dann ergiebt sich $2x = 3 + z^2$, $2y = z^2 - 3$. z muss also eine ungerade Zahl $2k + 1$ sein, und man erhält nach leichten Umformungen
$$x = (k^2 + 1) + (k+1)^2,\ y = (k^2 - 2) + (k+1)^2,\ z = 2k + 1\,.$$
Für $k = 2$ ist z. B. $x = 14$, $y = 11$, $z = 5$.

34) Zwei Zahlen zu bestimmen, deren Produkt, vermehrt um die Summe ihrer Quadrate, ein Quadrat gebe.

Setzt man $x^2 + xy + y^2 = (x+k)^2$, so erhält man leicht
$$x = -y - 2k + \frac{3k^2}{2k - y}\,.$$

k und y sind nur der Bedingung unterworfen, dass $2k - y$ in $3k^2$ aufgehe. Passende Werthe sind z. B.

k	2	3	4	5	6	...
y	3	5	7	9	11	...
x	5	16	33	56	85	...

35) Drei ganze Zahlen bilden eine arithmetische Reihe, und je zwei haben zur Summe eine Quadratzahl. Welches sind diese Zahlen?

Lösung. Werden die Zahlen mit

$$x, \; x + y, \; x + 2y$$

bezeichnet, so ist

$$2x + y = \alpha^2,$$
$$2x + 3y = \beta^2,$$
$$2x + 2y = \gamma^2,$$

also

$$\alpha^2 + \beta^2 = 2\gamma^2.$$

Nun ist bekanntlich

$$(u + v)^2 + (u - v)^2 = 2(u^2 + v^2),$$

also, wenn $\alpha = u + v$, $\beta = u - v$ gesetzt wird,

$$\gamma^2 = u^2 + v^2,$$

oder, wenn k eine unbestimmte ganze Zahl bezeichnet, nach § 29

$$u = 2k, \; v = 1 - k^2, \; \gamma = 1 + k^2.$$

Wir erhalten somit

$$\alpha = 1 + 2k - k^2,$$
$$\beta = -1 + 2k + k^2,$$
$$\gamma = 1 + k^2,$$

und aus den Werthen von α, β, γ ergeben sich sofort die von x, y.

Für $k = 3$ ist z. B. $x = -46$, $y = 96$, also die 3 gesuchten Zahlen

$$-46, \; 50, \; 146.$$

Für $k = 7$ sind dieselben

$$-94, \; 1250, \; 2594.$$

36) Eine Zahl x von solcher Beschaffenheit zu finden,

dass, wenn man eine gegebene Zahl a davon subtrahirt und dazu addirt, in beiden Fällen sich ein Quadrat ergiebt.

Lösung. Setzen wir

$$x + a = y^2,$$

so ist

$$x - a = y^2 - 2a.$$

Dieser Ausdruck soll ein Quadrat werden; wir setzen also

$$y^2 - 2a = (y - k)^2$$

und erhalten der Reihe nach

$$-2a = -2ky + k^2,$$

$$y = \frac{2a + k^2}{2k},$$

$$x = \left(\frac{2a + k^2}{2k}\right)^2 - a = \frac{4a^2 + k^4}{4k^2}.$$

Diese Zahl x genügt für jeden Werth von k der gestellten Aufgabe.

37) Die Gleichung $x^y = y^x$ aufzulösen (Euler, Introductio, II. p. 294).

Wird $y = tx$ angenommen, so ist

$$x^{tx} = (tx)^x,$$

also

$$x^t = tx,$$

$$x^{t-1} = t,$$

$$x = \sqrt[t-1]{t},$$

$$y = \sqrt[t-1]{t^t}.$$

Wenn wir jetzt $t - 1 = \frac{1}{u}$ setzen, so erhalten wir

$$x = \left(1 + \frac{1}{u}\right)^u, \quad y = \left(1 + \frac{1}{u}\right)^{u+1}.$$

Für $u = 1, 2, 3$ z. B. ist beziehungsweise

$$\begin{cases} x = 2 \\ y = 4 \end{cases}, \quad \begin{cases} x = \frac{9}{4} \\ y = \frac{27}{8} \end{cases}, \quad \begin{cases} x = \frac{64}{27} \\ y = \frac{256}{81} \end{cases}.$$

Siebentes Kapitel.

Congruenzen zweiten Grades.

§ 73. Verwandlung einer gemischt quadratischen Congruenz in eine rein quadratische. — Die allgemeine Congruenz zweiten Grades mit einer Unbekannten hat die Form

(1) $$ax^2 + bx + c \equiv 0 \pmod{m},$$

wo a, b, c positive oder negative ganze Zahlen bezeichnen, und lässt sich leicht in eine rein quadratische Congruenz von der Form

$$x^2 \equiv \alpha \pmod{\mu}$$

verwandeln, wo μ ein Vielfaches von m ist. Dieser Zweck wird in allen Fällen durch Multiplication der vorgelegten Congruenz mit $4a$ erreicht. Man erhält dadurch nämlich

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}$$

oder

$$(2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{4am},$$

d. h.

(2) $$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}.$$

Mittels dieser rein quadratischen Congruenz bestimmt man die Werthe ξ_1, ξ_2, ... des Ausdrucks $2ax + b$; darauf liefert jede der linearen Congruenzen

$$2ax + b \equiv \xi_1, \quad 2ax + b \equiv \xi_2, \quad \ldots \pmod{4am}$$

die etwa vorhandenen entsprechenden Werthe von x.

Wenn a prim zum Modul m ist, so lässt sich die Rechnung ein wenig abkürzen. In diesem Falle kann man nämlich eine Zahl α bestimmen, welche der Congruenz $a\alpha \equiv 1 \pmod{m}$ genügt, und durch Multiplication mit α wird der Coefficient von x^2 in (1) auf die Einheit reducirt.

Beispiel. Die Congruenz

$$7x^2 - 3x - 4 \equiv 0 \pmod{12}$$

liefert, wenn man sie mit 28 multiplicirt,

$$196x^2 - 84x - 112 \equiv 0 \pmod{336}$$

oder

$$(14x - 3)^2 \equiv 121 \pmod{336}.$$

Da $336 = 16 \cdot 3 \cdot 7$ ist, so hat man die Congruenz $(14x - 3)^2 \equiv 121$ für jeden der drei Moduln 16, 3, 7 aufzulösen. Wird $14x - 3$ der Kürze wegen mit y bezeichnet, so erhält man

$$y \equiv \pm 3, \pm 11 \pmod{16},$$
$$y \equiv \pm 1 \pmod{3},$$
$$y \equiv \pm 3 \pmod{7},$$

und durch Verbindung jedes der 4 ersten mit jedem der 2 zweiten mit jedem der 2 dritten Werthe ergeben sich im Ganzen folgende mod. 336 incongruenten 16 Werthe von y

$$\pm 115, \pm 59, \pm 53, \pm 67, \pm 11, \pm 101, \pm 157, \pm 109,$$

welche für x die vier mod. 12 incongruenten Werthe 1, 4, 5, 8 liefern.

Besser hätte man die vorgelegte Congruenz erst durch Multiplication mit 7 auf die einfachere Form

$$49x^2 - 21x - 28 \equiv 0 \pmod{12},$$

d. h.

$$x^2 - 9x - 4 \equiv 0 \pmod{12}$$

gebracht und dann durch Multiplication mit 4

$$(2x - 9)^2 \equiv 1 \pmod{48}$$

erhalten. Die Behandlung dieser Congruenz gemäss § 70 würde weniger unbrauchbare Werthe von y und die einzelnen brauchbaren weniger oft geliefert, also schneller zum Ziele geführt haben.

Die Unbequemlichkeit des dargelegten Verfahrens hat besonders darin ihren Grund, dass beim Uebergang von der Congruenz (1) zur Congruenz (2) auch der Modul vergrössert wird, und man durch Auflösung von (2) auch Werthe ermittelt, die sich als unbrauchbar erweisen, da zwar jede Wurzel von (1) auch (2) befriedigen muss, aber nicht umgekehrt jede Wurzel von (2) auch Wurzel von (1) zu sein hat. Diesen Uebelstand vermeidet man leicht, wenn der Modul eine Primzahl p ist. In diesem Falle ist der Coefficient a von x^2 nothwendig prim zu p, da sonst das Glied ax^2 fortfallen, die Congruenz (1) also eine lineare werden würde. Es

lässt sich also eine Zahl α bestimmen, welche der Congruenz $a\alpha \equiv 1 \pmod{p}$ genügt, und durch Multiplication mit α geht die vorgelegte Congruenz über in

$$\alpha a x^2 + \alpha b x + \alpha c \equiv 0 \pmod{p}.$$

αa hat den Rest 1; der Rest β von αb kann als eine gerade Zahl vorausgesetzt werden; denn wenn derselbe ungerade ist, so kann man ihn durch den geraden negativen Rest $-(p-\beta)$ ersetzen. Wir wollen diesen geraden Rest von αb mit 2β und den Rest von αc mit γ bezeichnen; dann geht die vorgelegte Congruenz über in

$$x^2 + 2\beta x + \gamma \equiv 0 \pmod{p}$$

oder

$$(x+\beta)^2 \equiv \beta^2 - \gamma \pmod{p}.$$

Beispiele. I. $5x^2 - 11x - 12 \equiv 0 \pmod{23}$

geht durch Multiplication mit 14 über in

$$70x^2 - 154x - 168 \equiv 0 \pmod{23}$$

oder

$$x^2 - 16x - 7 \equiv 0 \pmod{23},$$

$$(x-8)^2 \equiv 2 \pmod{23},$$

und man erhält leicht

$$x - 8 \equiv 5 \quad \text{oder} \quad -5 \pmod{23},$$

also

$$x \equiv 13 \quad \text{oder} \quad \equiv 3 \pmod{23}.$$

II. $x^2 - 3x - 6 \equiv 0 \pmod{12}$

geht durch Multiplication mit 4 über in

$$(2x-3)^2 \equiv 33 \pmod{48}.$$

Nun hat, wenn $2x - 3 = y$ gesetzt wird, die Congruenz $y^2 \equiv 33 \pmod{3}$ die Wurzel $y \equiv 0 \pmod{3}$ und die Congruenz $y^2 \equiv 33 \pmod{16}$ die 4 Wurzeln

$$y \equiv \pm 1, \quad \pm 7 \pmod{16}.$$

Es ergeben sich daraus für y die 4 Werthe ± 9, ± 15, welche für x die 2 nach dem Modul 12 incongruenten Wurzeln

$$x \equiv 6,\ 9 \pmod{12}$$

liefern.

Da nach dem Vorhergehenden jede Congruenz zweiten Grades mit einer Unbekannten auf die Form

$$x^2 \equiv a \pmod{m}$$

gebracht werden kann, so können wir für die folgenden Betrachtungen diese Form von vorn herein zu Grunde legen.

§ 74. Quadratische Reste und Nichtreste. — Die Congruenz

(1) $$x^2 \equiv a \pmod{m},$$

auf welche wir jede Congruenz zweiten Grades mit einer Unbekannten zurückführen können, ist nicht für alle Werthe, die man der Zahl a beilegen kann, möglich. Das sieht man, wenn der Modul m die Anwendung von Indices gestattet, durch Uebergang zu der Congruenz

(2) $$2 \text{ Ind. } x \equiv \text{Ind. } a \pmod{\varphi(m)};$$

da nämlich $\varphi(m)$ eine gerade Zahl ist, so kann diese Congruenz nur bestehen, wenn Ind. a gerade ist; also ist auch die Congruenz (1) nicht für alle Werthe von a möglich. Es lässt sich dies aber auch ohne Anwendung der Indices leicht darthun.

Betrachten wir nämlich die Reste, welche die Quadrate der Zahlen 0, 1, 2, 3, ... für irgend einen Modul m geben, so erkennen wir zunächst, dass congruente Zahlen auch congruente Quadrate liefern; um also alle für den Modul m möglichen Reste von Quadraten zu erhalten, können wir uns auf die Zahlen der Reihe

(3) $$0,\ 1,\ 2,\ 3,\ \ldots,\ (m-1)$$

beschränken, deren Quadrate die Reste

(4) $$0,\ 1,\ 4,\ \ldots$$

haben. Nun ist

$$(m-1)^2 = m^2 - 2m + 1 \equiv 1^2, \quad (m-2)^2 \equiv 2^2, \ \ldots,$$

allgemein

$$(m-k)^2 \equiv k^2 \pmod{m};$$

folglich lassen sich die Zahlen der Reihe (3) [abgesehen von 0 und bei geradem m von $\frac{m}{2}$] in Gruppen von je zweien zusammenfassen, so dass die Quadrate der beiden Zahlen jeder Gruppe denselben Rest liefern. Die Reihe (4) wird also einige Zahlen von (3) wiederholt, andere gar nicht enthalten. Die Zahlen (3), also überhaupt alle Zahlen, lassen sich danach in zwei Klassen theilen.

Die Zahlen der ersten Klasse sind nach dem Modul m einem Quadrate congruent, die Zahlen der zweiten Klasse

nicht, oder anders ausgedrückt, für eine Zahl a der ersten Klasse ist die Congruenz $x^2 \equiv a \pmod{m}$ möglich, für eine Zahl der zweiten Klasse nicht. Man nennt die Zahlen der ersten Klasse quadratische Reste von m, die der zweiten Klasse quadratische Nichtreste. Wo kein Missverständniss zu befürchten ist, sagt man auch einfach Reste und Nichtreste von m.

Beispiele. I. Für den Modul $m = 11$ sind die Quadrate der Zahlen $0, 1, 2, 3, \ldots, 10$ beziehungsweise den Zahlen $0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1$ congruent; daher sind $0, 1, 3, 4, 5, 9$ die Reste, $2, 6, 7, 8, 10$ die Nichtreste von 11.

Die Zahl 10 hat die Reste $0, 1, 4, 5, 6, 9$, die Nichtreste $2, 3, 7, 8$.

Anmerkung. Um eine einfache Fassung der Sätze zu ermöglichen, schliessen wir die Zahl 0, welche immer Rest ist, und die Zahlen, welche nicht prim zum Modul sind, vorläufig von der Betrachtung aus.

§ 75. Reste einer ungeraden Primzahl. —

Satz. Wenn der Modul p eine ungerade Primzahl ist, so enthält die Reihe $1, 2, 3, \ldots, p-1$ ebenso viele Reste wie Nichtreste.

1. **Beweis.** Es sei g eine primitive Wurzel von p, so lassen sich nach dem Früheren die Zahlen $1, 2, 3, \ldots, p-1$ durch die Potenzen $g, g^2, \ldots, g^{p-1}$ ersetzen, und jede Potenz von g, deren Exponent eine gerade Zahl ist, ist ein Rest, jede andere ein Nichtrest von p. Da nun $p-1$ gerade ist, so ist die Hälfte jener Potenzen von der ersten, die andere Hälfte von der zweiten Art, d. h. p besitzt $\frac{p-1}{2}$ Reste und ebenso viele Nichtreste

2. **Beweis.** Es sei $p = 2n + 1$, so haben wir die Zahlen

$$1, 2, 3, \ldots, n, n+1, n+2, \ldots, 2n$$

zu betrachten. Die Quadrate der n ersten dieser Zahlen sind nach dem Modul p incongruent; denn, wenn a, b zwei Zahlen der Reihe $1, 2, \ldots, n$ bezeichnen, so ist die Congruenz

$$a^2 \equiv b^2, \quad \text{d. i.} \quad a^2 - b^2 \equiv 0$$

oder

$$(a+b)(a-b) \equiv 0 \pmod{p}$$

nur unter der Voraussetzung $a = b$ möglich. Dagegen geben die Quadrate der n folgenden Zahlen $n + 1, \ldots, 2n$ wieder dieselben Reste (in umgekehrter Reihenfolge), da

$$(n + 1)^2 - n^2 = 2n + 1 = p \equiv 0 \pmod{p},$$
$$(n + 2)^2 - (n - 1)^2 = 6n + 3 = 3p \equiv 0 \pmod{p},$$

allgemein

$$(n + \alpha)^2 - (n - [\alpha - 1])^2 = 2n(2\alpha - 1) + (2\alpha - 1)$$
$$= (2\alpha - 1)p \equiv 0 \pmod{p} \text{ ist.}$$

Ist a ein Rest von p, so ist die Congruenz

$$x^2 \equiv a \pmod{p}$$

möglich, und wenn eine Wurzel derselben mit α bezeichnet wird, so ist eine zweite Wurzel $-\alpha \equiv p - \alpha \pmod{p}$, da, wenn $\alpha^2 \equiv a$ ist, auch $(-\alpha)^2 \equiv a$ sein wird. Mehr als zwei Wurzeln kann aber die Congruenz, da p eine Primzahl ist, nicht besitzen, und somit sind $\pm \alpha$ ihre einzigen Wurzeln.

§ 76. Reste einer Potenz einer ungeraden Primzahl. — **Lehrsatz I.** Die Hälfte der Zahlen, die prim zu p^λ und nicht grösser als p^λ sind, sind Reste von p^λ, die Hälfte Nichtreste.

Beweis. Hie Hälfte der $\varphi(p^\lambda) = (p - 1)p^{\lambda - 1}$ Zahlen, welche prim zu p^λ und nicht grösser als p^λ sind, sind kleiner als der halbe Modul, die Hälfte grösser. Es lässt sich nun zeigen, dass die Quadrate derjenigen dieser Zahlen, die kleiner als der halbe Modul sind, incongruent sein müssen. Sind nämlich a, b zwei solche Zahlen, so würde aus der Annahme $a^2 \equiv b^2 \pmod{p^\lambda}$ sich die Congruenz

$$(a + b)(a - b) \equiv 0 \pmod{p^\lambda}$$

ergeben. Es müsste also entweder eine der Zahlen $a + b$, $a - b$ durch p^λ theilbar sein, was unmöglich ist, da sowohl a, als auch $b < \frac{1}{2}p^\lambda$ ist, daher $a + b$, wie auch $a - b$ kleiner als p^λ sein muss; oder es müsste $a + b$ durch eine Potenz p^k von p und $a - b$ durch $p^{\lambda - k}$ theilbar sein. Dies ist aber gleichfalls unmöglich; denn sonst würde jede der Zahlen $a + b$, $a - b$, also auch ihre Summe $2a$ und ihre Differenz $2b$ und, da 2 prim zu p ist, a und b durch p theilbar sein, was der Voraussetzung widerspricht. Die Quadrate der $\frac{1}{2}\varphi(p^\lambda)$ Zahlen,

welche prim zu p und kleiner als $\frac{1}{2}p^\lambda$ sind, sind daher sämmtlich incongruent.

Da nun die Quadrate der $\frac{1}{2}\varphi(p^\lambda)$ folgenden Zahlen der Relation $(p^\lambda - a)^2 \equiv a^2 \pmod{p^\lambda}$ wegen wieder dieselben Reste liefern, so sehen wir, dass auch in diesem Falle die Zahl der Reste gleich der der Nichtreste, nämlich $\frac{1}{2}\varphi(p^\lambda)$ ist.

Anmerkung. Wir überlassen es dem Leser, den Satz durch Benutzung der Indices zu beweisen.

Lehrsatz II. Jeder Rest von p ist auch Rest von p^λ, jeder Nichtrest von p auch Nichtrest von p^λ.

Beweis. Die Zahlen, welche prim zu p und nicht grösser als p^λ sind, lassen sich in folgende $p^{\lambda-1}$ Reihen stellen:

$$1,\ 2,\ 3,\ \ldots,\ (p-1),$$
$$p+1,\ p+2,\ p+3,\ \ldots,\ (2p-1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$p^\lambda - p + 1,\ p^\lambda - p + 2,\ p^\lambda - p + 3,\ \ldots,\ (p^\lambda - 1).$$

Da nun die Congruenz $x^2 \equiv a$, wenn sie für den Modul p unmöglich ist, gewiss auch für den Modul p^λ unmöglich sein wird, da also ein Nichtrest von p auch ein Nichtrest von p^λ ist, so müssen alle Reste von p^λ sich unter den Resten von p vorfinden. Nun besitzt p in jeder der obigen Reihen $\frac{p-1}{2}$ Reste, also in allen Reihen zusammen $\frac{1}{2}(p-1)p^{\lambda-1}$ Reste. Wäre einer dieser Reste Nichtrest von p^λ, so würde p^λ weniger als $\frac{1}{2}(p-1)p^{\lambda-1}$ Reste haben, was dem vorhergehenden Satze widerspricht. Es ist also auch jeder Rest von p ein Rest von p^λ.

Aufgabe. Es sind die beiden Wurzeln $\pm a$ der Congruenz $x^2 \equiv r \pmod{p}$ gegeben. Man soll daraus die Wurzeln der Congruenz $x^2 \equiv r \pmod{p^\lambda}$ herleiten.

Wir behandeln zunächst die Congruenz $x^2 \equiv r \pmod{p^2}$, deren Wurzeln offenbar von der Form $\pm a + py$ sein müssen. Es ist nun

$$(\pm a + py)^2 = a^2 \pm 2apy + p^2y^2$$

oder, da dieser Ausdruck $\equiv r \pmod{p^2}$ sein soll,

$$a^2 \pm 2apy \equiv r \pmod{p^2}.$$

Nun ist aber $a^2 \equiv r \pmod{p}$, also etwa $a^2 = r + kp$,

und durch Einsetzung dieses Werthes geht die vorhergehende Congruenz über in

$$kp \pm 2apy \equiv 0 \pmod{p^2}$$

oder

$$k \pm 2ay \equiv 0 \pmod{p}.$$

Da $2a$ prim zu p ist, so ist diese Congruenz stets möglich und liefert, des Zeichens $\pm$ wegen, zwei Werthe von y, einen, welcher dem oberen und einen zweiten, welcher dem unteren Zeichen entspricht, so dass wir für die Congruenz

$$x^2 \equiv r \pmod{p^2}$$

zwei Lösungen $\pm b$ erhalten.

Um weiter die Congruenz $x^2 \equiv r \pmod{p^3}$ zu lösen, deren Wurzeln von der Form $\pm b + p^2 y$ sein werden, setzen wir

$$(\pm b + p^2 y)^2 \equiv r \pmod{p^3}$$

und erhalten

$$b^2 \pm 2bp^2 y + p^4 y^2 \equiv r \pmod{p^3}$$

oder, weil $b^2 \equiv r \pmod{p^2}$, etwa $b^2 = r + k'p^2$ ist,

$$k' \pm 2by \equiv 0 \pmod{p}.$$

Hieraus ergeben sich wieder zwei Werthe von y, welche zu zwei Lösungen der vorgelegten Congruenz führen.

So fortfahrend löst man die Congruenz $x^2 \equiv r \pmod{p^\lambda}$ für jeden gegebenen Werth von λ und überzeugt sich zugleich, dass dieselbe immer zwei Wurzeln besitzt, wofern nur r ein Rest von p ist.

Beispiel. Die Congruenz $x^2 \equiv 2 \pmod{7}$ hat die beiden Wurzeln ± 3. Es soll die Congruenz

$$x^2 \equiv 2 \pmod{7^4}$$

gelöst werden. Wir setzen zunächst

$$(\pm 3 + 7y)^2 \equiv 2 \pmod{7^2}$$

und erhalten der Reihe nach

$$\pm 42y \equiv -7 \pmod{7^2},$$

$$\pm 6y \equiv -1 \equiv 6 \pmod{7},$$

$$y \equiv \pm 1 \pmod{7},$$

$$\pm 3 + 7y \equiv \pm 3 \pm 7 \equiv \pm 10 \pmod{7^2}.$$

± 10 sind also die Wurzeln der Congruenz $x^2 \equiv 2 \pmod{7^2}$.

Weiter setzen wir

$$(\pm 10 + 7^2 y)^2 \equiv 2 \pmod{7^3}$$

und erhalten

$$\pm 20 \cdot 7^2 \cdot y \equiv -98 \pmod{7^3},$$

$$\pm 20 y \equiv -2 \pmod{7},$$

$$y \equiv \pm 2 \pmod{7},$$

$$\pm 10 + 7^2 y \equiv \pm 10 \pm 98 \equiv \pm 108 \pmod{7^3}.$$

± 108 sind also die Wurzeln von $x^2 \equiv 2 \pmod{7^3}$.

Endlich setzen wir

$$(\pm 108 + 7^3 y)^2 \equiv 2 \pmod{7^4}$$

und erhalten

$$\pm 216 \cdot 7^3 y \equiv -11662 \pmod{7^4},$$

$$\pm 216 y \equiv -34 \pmod{7},$$

$$y \equiv \mp 1 \pmod{7},$$

$$\pm 108 + 7^3 y \equiv \pm 108 \mp 343 = \mp 235;$$

also sind ± 235 die Wurzeln der Congruenz

$$x^2 \equiv 2 \pmod{7^4}.$$

§ 77. Mittel zu entscheiden, ob eine gegebene Zahl Rest oder Nichtrest einer ungeraden Primzahl oder einer Potenz einer solchen sei.

Lehrsatz I. Für jede beliebige primitive Wurzel von p^λ, wo p eine ungerade Primzahl und λ eine ganze positive Zahl ist, hat die Zahl $p^\lambda - 1$ den Index $\frac{1}{2}\varphi(p^\lambda)$.

Beweis. Wird die primitive Wurzel mit g und der Index von $p^\lambda - 1$ mit x bezeichnet, so ist

$$g^x \equiv p^\lambda - 1 \equiv -1 \pmod{p^\lambda},$$

also

$$g^{2x} \equiv +1 \pmod{p^\lambda}.$$

Daher muss nach dem Fermat'schen Satze $2x$ ein Vielfaches von $\varphi(p^\lambda)$, also x ein Vielfaches von $\frac{1}{2}\varphi(p^\lambda)$ sein. Es ist somit

$$x \equiv \tfrac{1}{2}\varphi(p^\lambda) \; [\text{mod.}\ \varphi(p^\lambda)].$$

Lehrsatz II (Umkehrung). Die Zahl, welche den Index $\frac{1}{2}\varphi(p^\lambda)$ hat, ist $p^\lambda - 1$.

Beweis. Wird die Zahl, deren Index für eine primitive Wurzel g gleich $\frac{1}{2}\varphi(p^\lambda)$ ist, mit x bezeichnet, ist also

$$g^{\frac{1}{2}\varphi(p^\lambda)} \equiv x \pmod{p^\lambda},$$

so ergiebt sich $g^{\varphi(p^\lambda)} \equiv x^2$ oder, da $g^{\varphi(p^\lambda)} \equiv 1$ ist,

$$x^2 \equiv 1 \pmod{p^\lambda}.$$

Diese Congruenz hat die beiden Wurzeln ± 1, und da sie nach dem vorigen Paragraphen überhaupt nur zwei Wurzeln besitzt, so sind dies ihre einzigen Wurzeln. Es kann aber x nicht $\equiv +1$ sein, da g eine primitive Wurzel von p^λ ist, also erst die $\varphi(p^\lambda)^{\text{te}}$, nicht schon die $\frac{1}{2}\varphi(p^\lambda)^{\text{te}}$ Potenz von g den Rest $+1$ geben kann. Daher ist

$$x \equiv -1 \equiv p^\lambda - 1 \pmod{p^\lambda}.$$

Lehrsatz III. Bezeichnet a einen Rest, b einen Nichtrest von p^λ, so ist

$$a^{\frac{1}{2}\varphi(p^\lambda)} \equiv +1, \quad b^{\frac{1}{2}\varphi(p^\lambda)} \equiv -1 \pmod{p^\lambda}.$$

Beweis. Da a ein Rest sein soll, so ist sein Index eine gerade Zahl $2m$, also

$$a \equiv g^{2m} \pmod{p^\lambda},$$

und daraus folgt

$$a^{\frac{1}{2}\varphi(p^\lambda)} \equiv g^{m\varphi(p^\lambda)} \equiv +1 \pmod{p^\lambda}.$$

Da andererseits b ein Nichtrest sein soll, so ist sein Index eine ungerade Zahl $2m+1$, und aus der Annahme

$$b \equiv g^{2m+1} \equiv g^{2m} \cdot g \pmod{p^\lambda}$$

folgt

$$b^{\frac{1}{2}\varphi(p^\lambda)} \equiv g^{m\varphi(p^\lambda)} \cdot g^{\frac{1}{2}\varphi(p^\lambda)} \equiv -1 \pmod{p^\lambda}.$$

Lehrsatz IV. (Umkehrung). Eine Zahl a ist Rest oder Nichtrest von p^λ, je nachdem

$$a^{\frac{1}{2}\varphi(p^\lambda)} \equiv +1 \text{ oder } \equiv -1 \pmod{p^\lambda} \text{ ist.}$$

Beweis. Wird der Index von a für die primitive Wurzel g mit x bezeichnet, so ist

$$a \equiv g^x \pmod{p^\lambda},$$

also

$$a^{\frac{1}{2}\varphi(p^\lambda)} \equiv g^{\frac{x}{2}\varphi(p^\lambda)} \pmod{p^\lambda}.$$

Ist dieser Ausdruck $\equiv +1$, so ist $\frac{x}{2}\varphi(p^\lambda)$ ein Viel-

faches von $\varphi(p^\lambda)$, also $\frac{x}{2}$ ein Vielfaches von 1, d. h. x eine gerade Zahl und a ein Rest von p^λ.

Ist dagegen $g^{\frac{x}{2}\varphi(p^\lambda)} \equiv -1$, so muss x ungerade, also a ein Nichtrest sein, da die Annahme, x sei gerade,

$$g^{\frac{x}{2}\varphi(p^\lambda)} \equiv +1$$

liefern würde.

Der letzte Satz lehrt entscheiden, ob eine vorgelegte Zahl Rest oder Nichtrest einer ungeraden Primzahl oder einer Potenz einer solchen sei. Freilich führt seine Anwendung zu so grossen Zahlen, dass er praktisch kaum brauchbar ist.

Man beachte, dass $\frac{1}{2}\varphi(p^\lambda) = \frac{1}{2}(p-1)p^{\lambda-1}$ und, wenn $\lambda = 1$, $\frac{1}{2}\varphi(p) = \frac{p-1}{2}$ ist.

Den für den Modul p^λ genommenen Rest des Ausdrucks $a^{\frac{1}{2}\varphi(p^\lambda)}$ bezeichnet man nach Legendre (Théorie des nombres, II. partie, 135) durch das Symbol $\left(\frac{a}{p^\lambda}\right)$; dasselbe hat also den Werth $+1$ oder -1, je nachdem a Rest oder Nichtrest von p^λ ist.

§ 78. Produkte von Resten und Nichtresten. — Ob eine zusammengesetzte Zahl Rest oder Nichtrest einer ungeraden Primzahl oder einer Potenz einer solchen sei, hängt von der Beschaffenheit ihrer Factoren ab. Die Frage entscheidet immer der folgende

Lehrsatz. Das Produkt zweier Reste einer ungeraden Primzahl oder einer Potenz einer solchen ist ein Rest, das Produkt eines Restes in einen Nichtrest ein Nichtrest, das Produkt zweier Nichtreste endlich ist ein Rest.

1. **Beweis.** Es seien erstens a und b zwei Reste von p^λ, etwa $\alpha^2 \equiv a$, $\beta^2 \equiv b$, so ist $(\alpha\beta)^2 \equiv ab \pmod{p^\lambda}$, d. h. ab ein Rest von p^λ.

Zweitens sei a ein Rest, b ein Nichtrest von p^λ. Sind dann $\alpha, \beta, \gamma, \ldots, \delta$ sämmtliche $\frac{1}{2}\varphi(p^\lambda)$ Reste von p^λ, so sind die Produkte $a\alpha$, $a\beta$, $a\gamma$, $\ldots$, $a\delta$ sämmtlich incongruent, und jedes ist nach dem ersten Theil des Satzes ein Rest;

daher besitzt p^λ keinen Rest, der sich nicht unter diesen Produkten vorfindet. Da nun ab keinem dieser Produkte congruent sein kann, so ist ab ein Nichtrest.

Drittens seien a und b Nichtreste. Werden dann alle Reste von p^λ mit a multiplicirt, so stellen die erhaltenen Produkte $a\alpha$, $a\beta$, $a\gamma$, ..., $a\delta$ sämmtliche Nichtreste von p^λ dar, und da ab keinem dieser Produkte congruent sein kann, so muss ab ein Rest sein.

2. Beweis. Es sei g eine primitive Wurzel von p^λ und $a \equiv g^\alpha$, $b \equiv g^\beta$, so ist

$$ab \equiv g^{\alpha+\beta} \pmod{p^\lambda}.$$

Sind nun a und b Reste, also α, β gerade Zahlen, so ist auch $\alpha + \beta$ gerade, d. h. ab ein Rest. Ist a ein Rest, b ein Nichtrest, so ist α gerade, β ungerade, also $\alpha + \beta$ ungerade, d. h. ab ein Nichtrest. Wenn endlich a und b Nichtreste, also α und β ungerade sind, so ist $\alpha + \beta$ gerade, d. h. ab ein Rest.

3. Beweis. Es ist

$$a^{\frac{1}{2}\varphi(p^\lambda)} \cdot b^{\frac{1}{2}\varphi(p^\lambda)} = (ab)^{\frac{1}{2}\varphi(p^\lambda)},$$

und dies Produkt hat für den Modul p^λ den Rest $+1$, wenn jeder Factor $\equiv +1$ oder $\equiv -1$ ist; das Produkt ist dagegen $\equiv -1$, wenn der eine Factor $\equiv +1$, der andere $\equiv -1$ ist.

Der eben bewiesene Satz lässt sich in folgender Weise verallgemeinern:

Ein Produkt ist Rest oder Nichtrest von p^λ, je nachdem es eine gerade oder ungerade Anzahl von Factoren enthält, die Nichtreste sind.

Anmerkung. Bei Anwendung des Legendre'schen Symbols wird dieser Satz durch die Formel

$$\left(\frac{ab\ldots c}{p^\lambda}\right) = \left(\frac{a}{p^\lambda}\right)\left(\frac{b}{p^\lambda}\right)\cdots\left(\frac{c}{p^\lambda}\right)$$

ausgedrückt.

Beispiel. Die Zahl 49 hat die Reste

(1) 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29,
30, 32, 36, 37, 39, 43, 44, 46,

die Nichtreste

(2) 3, 5, 6, 10, 12, 13, 17, 19, 20, 24, 26, 27,
31, 33, 34, 38, 40, 41, 45, 47, 48.

Man überzeugt sich leicht, dass man durch Multiplication zweier Glieder der Reihe (1) wieder ein Glied von (1), durch Multiplication eines Gliedes von (1) mit einem Gliede von (2) stets ein Glied von (2), endlich durch Multiplication zweier Glieder von (2) ein Glied von (1) erhält.

§ 79. Reste der Potenzen von 2. — Für den Modul 2 ist jede ungerade Zahl $\equiv 1$, also ein Rest. Nichtreste giebt es in diesem Falle nicht, und die Congruenz $x^2 \equiv 1 \pmod{2}$ hat die eine Wurzel $+1 \equiv -1 \pmod{2}$.

Wenn der Modul 4 ist, so müssen, da a als prim zum Modul vorausgesetzt wird, die Wurzeln der Congruenz

$$x^2 \equiv a \pmod{4}$$

ungerade sein. Nun ist für jede ungerade Zahl $2n + 1$

$$(2n + 1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod{4},$$

und daher ist a Rest von 4, wenn es die Form $4n + 1$ hat; in diesem Falle hat die Congruenz $x^2 \equiv a \pmod{4}$ zwei Wurzeln, nämlich $+1$ und -1. Wenn a von der Form $4n + 3$ ist, so ist es Nichtrest von 4.

Da weiter

$$(4n \pm 1)^2 = 16n^2 \pm 8n + 1 \equiv 1 \pmod{8}$$

ist, also das Quadrat jeder ungeraden Zahl für den Modul 8 den Rest 1 giebt, so ist die Congruenz $x^2 \equiv a \pmod{8}$ nur möglich, wenn a die Form $8n + 1$ hat. Es sind also die Zahlen der Form $8n + 1$ Reste, die Zahlen der Formen $8n + 3$, $8n + 5$, $8n + 7$ Nichtreste von 8, und wenn $a \equiv 1 \pmod{8}$ ist, so hat die Congruenz $x^2 \equiv a \pmod{8}$ die vier Wurzeln ± 1, ± 3.

Endlich wollen wir noch die Congruenz

$$x^2 \equiv a \pmod{2^\varkappa}$$

betrachten, in welcher $\varkappa > 3$ vorausgesetzt wird. Dieselbe ist nur möglich, wenn zugleich die Congruenz $x^2 \equiv a \pmod{8}$ möglich ist, wenn also a die Form $8n + 1$ hat. Wir wollen jetzt zeigen, dass diese Bedingung nicht bloss erforderlich, sondern auch hinreichend ist, d. h. dass jede Zahl $8n + 1$ Rest von $2^\varkappa$ ist. Wir führen diesen Beweis, indem wir zeigen,

dass die Zahl a Rest von $2^{\nu+1}$ ist, wenn sie Rest von 2^{ν} ist. Es sei also α eine Wurzel der Congruenz $x^2 \equiv a \pmod{2^{\nu}}$, etwa $\alpha^2 = a + k \cdot 2^{\nu}$, wo k eine ganze Zahl bezeichnet.

Setzen wir dann $x = \alpha + 2^{\nu-1}y$, so ergiebt sich

$$x^2 = \alpha^2 + 2^{\nu}\alpha y + 2^{2\nu-2}y^2 = a + k \cdot 2^{\nu} + 2^{\nu}\alpha y + 2^{2\nu-2}y^2.$$

Soll nun die Congruenz $x^2 \equiv a \pmod{2^{\nu+1}}$ bestehen, so muss, da hier $2\nu - 2 > \nu + 1$ ist,

$$a + k \cdot 2^{\nu} + 2^{\nu}\alpha y \equiv a \pmod{2^{\nu+1}}$$

oder

$$k + \alpha y \equiv 0 \pmod{2}$$

sein. Da α ungerade ist, so ist diese Congruenz stets möglich und hat eine einzige Wurzel. Jede Wurzel der Congruenz $x^2 \equiv a \pmod{2^{\nu}}$ liefert also eine Wurzel derselben Congruenz für den Modul $2^{\nu+1}$, oder a ist Rest von $2^{\nu+1}$, wenn es Rest von 2^{ν} ist. Da nun jede Zahl $8n + 1$ Rest von 2^3 ist, so ist sie auch Rest von 2^4, u. s. w., allgemein von $2^{\varkappa}$, wo $\varkappa > 3$ vorausgesetzt wird. Nun ist $\frac{1}{4}$ der unter $2^{\varkappa}$ liegenden $2^{\varkappa-1}$ ungeraden Zahlen von der Form $8n + 1$; daher hat $2^{\varkappa}$ in dem betrachteten Falle $2^{\varkappa-3}$ Reste und $3 \cdot 2^{\varkappa-3}$ Nichtreste.

Da die Congruenz $x^2 \equiv a \pmod{8}$, wenn sie überhaupt möglich ist, vier Wurzeln besitzt, und da jede derselben eine Wurzel der Congruenz $x^2 \equiv a \pmod{16}$ liefert, so erkennen wir, dass auch letztere und allgemein jede Congruenz $x^2 \equiv a \pmod{2^{\varkappa}, \varkappa > 3}$ vier Wurzeln besitzt. Die Ermittlung derselben bietet nach dem Vorhergehenden keine Schwierigkeit.

Aufgabe. Es soll die Congruenz $x^2 \equiv 33 \pmod{256}$ gelöst werden.

I. $x^2 \equiv 33 \pmod{8}$ hat die Wurzeln ± 1, ± 3.

Für $\alpha = \pm 1$ ist $\alpha^2 = 1 = 33 - 4 \cdot 8$, also $k = -4$.

Wird dann $x = \pm 1 + 4y$ gesetzt, so erfordert die Congruenz $(\pm 1 + 4y)^2 \equiv 33 \pmod{16}$, dass

$$-4 \pm y \equiv 0 \pmod{2},$$

also $y \equiv 0 \pmod{2}$, $x \equiv \pm 1 \pmod{8}$ sei.

Für $\alpha = \pm 3$ ist $\alpha^2 = 9 = 33 - 3 \cdot 8$, also $k = -3$.

Wird dann $x = \pm 3 + 4y$ gesetzt, so ergiebt sich aus der Congruenz $(\pm 3 + 4y)^2 \equiv 33 \pmod{16}$, dass

$$-3 \pm 3y \equiv 0 \pmod{2},$$

also $y \equiv \pm 1 \pmod{2}$ und $x \equiv \pm 3 \pm 4 \equiv \pm 7 \pmod{8}$ ist.

Die Congruenz $x^2 \equiv 33 \pmod{16}$ hat also die Wurzeln $\pm 1, \pm 7$.

II. $\alpha = \pm 1, \; \alpha^2 = 1 = 33 - 2 \cdot 16, \; k = -2.$

$x = \pm 1 + 8y, \; -2 \pm y \equiv 0 \pmod{2},$

$y \equiv 0 \pmod{2}, \; x \equiv \pm 1 \pmod{16}.$

$\alpha = \pm 7, \; \alpha^2 = 49 = 33 + 1 \cdot 16, \; k = 1.$

$x = \pm 7 + 8y, \; 1 \pm 7y \equiv 0 \pmod{2},$

$y \equiv \pm 1 \pmod{2}, \; x \equiv \pm 7 \pm 8 \equiv \pm 15 \pmod{16}.$

Die Wurzeln der Congruenz $x^2 \equiv 33 \pmod{32}$ sind also $\pm 1, \pm 15$.

III. $\alpha = \pm 1, \; \alpha^2 = 1 = 33 - 1 \cdot 32, \; k = -1.$

$x = \pm 1 + 16y, \; -1 \pm y \equiv 0 \pmod{2},$

$y \equiv \pm 1 \pmod{2}, \; x \equiv \pm 1 \pm 16 \equiv \pm 17 \pmod{32}.$

$\alpha = \pm 15, \; \alpha^2 = 225 = 33 + 6 \cdot 32, \; k = 6.$

$x = \pm 15 + 16y, \; 6 \pm 15y \equiv 0, \; y \equiv 0 \pmod{2},$

$x \equiv \pm 15 \pmod{32}.$

Die Wurzeln der Congruenz $x^2 \equiv 33 \pmod{64}$ sind also $\pm 17, \pm 15$.

IV. $\alpha = \pm 17, \; \alpha^2 = 289 = 33 + 4 \cdot 64, \; k = 4.$

$x = \pm 17 + 32y, \; 4 \pm 17y \equiv 0, \; y \equiv 0 \pmod{2},$

$x \equiv \pm 17 \pmod{64}.$

$\alpha = \pm 15, \; \alpha^2 = 225 = 33 + 3 \cdot 64, \; k = 3.$

$x = \pm 15 + 32y, \; 3 \pm 15y \equiv 0, \; y \equiv \pm 1 \pmod{2},$

$x \equiv \pm 15 \pm 32 \equiv \pm 47 \pmod{64}.$

Die Wurzeln der Congruenz $x^2 \equiv 33 \pmod{128}$ sind also $\pm 17, \pm 47$.

V. $\alpha = \pm 17, \; \alpha^2 = 289 = 33 + 2 \cdot 128, \; k = 2.$

$x = \pm 17 + 64y, \; 2 \pm 17y \equiv 0, \; y \equiv 0 \pmod{2},$

$x \equiv \pm 17 \pmod{128}.$

$\alpha = \pm 47, \; \alpha^2 = 2209 = 33 + 17 \cdot 128, \; k = 17.$

$x = \pm 47 + 64y, \; 17 \pm 47y \equiv 0, \; y \equiv \pm 1 \pmod{2},$

$x \equiv \pm 47 \pm 64 \equiv \pm 111 \pmod{128}.$

Also hat die Congruenz

$$x^2 \equiv 33 \pmod{256}$$

die 4 Wurzeln ± 17, ± 111.

§ 80. Reste eines beliebig zusammengesetzten Moduls. — Wenn der Modul $m = 2^\varkappa p^\lambda q^\mu \ldots$ ist, wo $p, q, \ldots$ ungerade Primzahlen, $\varkappa, \lambda, \mu, \ldots$ ganze positive Zahlen bezeichnen, so muss offenbar eine Zahl a, welche Rest von m ist, auch Rest jeder der Zahlen $2^\varkappa, p^\lambda, q^\mu, \ldots$ sein. Wenn also die Zahl a Nichtrest einer einzigen der Zahlen $2^\varkappa, p^\lambda, \ldots$ ist, so ist sie auch Nichtrest von m. Wenn a umgekehrt Rest jeder der Zahlen $2^\varkappa, p^\lambda, \ldots$ ist, so muss sie auch Rest von m sein. Es sei nämlich

$$\alpha^2 \equiv a \pmod{2^\varkappa},$$
$$\beta^2 \equiv a \pmod{p^\lambda},$$
$$\ldots\ldots\ldots;$$

wird dann eine Zahl ξ bestimmt, welche den Bedingungen

$$\xi \equiv \alpha \pmod{2^\varkappa}, \quad \xi \equiv \beta \pmod{p^\lambda}, \ldots$$

genügt, so ist

$$\xi^2 \equiv \alpha^2 \equiv a \pmod{2^\varkappa}, \quad \xi^2 \equiv \beta^2 \equiv a \pmod{p^\lambda}, \ldots;$$

also ist $\xi^2 - a$ durch jede der Zahlen $2^\varkappa, p^\lambda, \ldots$, und, da letztere prim zu einander sind, auch durch das Produkt derselben theilbar, d. h. es ist

$$\xi^2 \equiv a \pmod{m}.$$

Um also zu erkennen, ob eine Zahl a Rest von m sei, hat man zu untersuchen, ob sie Rest jedes Primfactors von m ist. Nur wenn dies der Fall ist, ist sie auch Rest von m.

Es ist nun auch leicht anzugeben, wie viele Wurzeln die Congruenz

$$x^2 \equiv a \pmod{2^\varkappa p^\lambda q^\mu \ldots}$$

besitzt.

Die Congruenz $x^2 \equiv a \pmod{2^\varkappa}$ hat, je nachdem $\varkappa = 1, = 2, > 2$ ist, 1, 2 oder 4 Wurzeln. Jede der folgenden Congruenzen, die wir zu lösen haben, $x^2 \equiv a \pmod{p^\lambda}, \ldots$ hat 2 Wurzeln, und solcher Congruenzen sind k vorhanden, wenn k ausdrückt, wie viele ungerade Primzahlen $p, q, \ldots$ in m enthalten sind. Da wir nun, um alle Wurzeln der vorgelegten Congruenz zu erhalten, jede Wurzel der ersten Congruenz mit

jeder Wurzel der zweiten, mit jeder Wurzel der dritten, u. s. w. in der angegebenen Weise zu combiniren haben, so erkennen wir, dass die Congruenz

$$x^2 \equiv a \pmod{2^\varkappa p^\lambda q^\mu \ldots}$$

2^k, $2 \cdot 2^k = 2^{k+1}$ oder $4 \cdot 2^k = 2^{k+2}$ Wurzeln besitzt, je nachdem $\varkappa = 1$, $= 2$ oder > 2 ist.

Aufgaben. 1) $x^2 \equiv 13 \pmod{54}$ [± 11]

2) $x^2 \equiv 137 \pmod{196}$ [± 23, ± 75]

3) $x^2 \equiv -191 \pmod{1296}$ [± 49, ± 113, ± 535, ± 599]

4) $x^2 \equiv 1 \pmod{210}$ [± 1, ± 29, ± 41, ± 71]

5) $x^2 \equiv 55 \pmod{95}$ [± 25, ± 70]

6) $x^2 \equiv -11 \pmod{5575 = 25 \cdot 223}$ [± 1883, ± 1908]

7) $x^2 \equiv 121 \pmod{552 = 2^3 \cdot 3 \cdot 23}$

[± 11, ± 35, ± 103, ± 127, ± 149, ± 173, ± 241, ± 265]

8) $x^2 \equiv 5 \pmod{844 = 4 \cdot 211}$ [± 65, ± 357].

§ 81. Der verallgemeinerte Wilson'sche Satz. — Das Produkt aller Zahlen, welche prim zu m und nicht grösser als m sind, ist $\equiv -1 \pmod{m}$, wofern m primitive Wurzeln besitzt; in allen anderen Fällen ist dasselbe $\equiv +1 \pmod{m}$.

Beweis. Die Zahlen, welche prim zu m und nicht grösser als m sind, lassen sich in zwei Klassen zerlegen; die erste Klasse enthalte diejenigen dieser Zahlen, welche der Congruenz $x^2 \equiv 1 \pmod{m}$ genügen, die zweite die übrigen.

Was nun die Zahlen der zweiten Klasse betrifft, so kann man dieselben in Paare von je zweien ordnen, so dass das Produkt der Zahlen jedes Paares $\equiv 1 \pmod{m}$ sei. Wenn nämlich a eine Zahl der zweiten Klasse ist, so lässt sich stets eine und nur eine Zahl b bestimmen, welche der Congruenz $ab \equiv 1 \pmod{m}$ genügt, und diese Zahl muss von a verschieden sein, da a sonst der Voraussetzung zuwider in die erste Klasse gehören würde. Das Produkt aller Zahlen der zweiten Klasse ist daher $\equiv 1 \pmod{m}$, und somit hat das Produkt aller Zahlen, welche prim zu m und nicht grösser als m sind, für den Modul m denselben Rest, wie das Produkt

aller Zahlen der ersten Klasse, d. i. das Produkt aller Wurzeln der Congruenz $x^2 \equiv 1 \pmod{m}$.

Diese letzteren lassen sich nun gleichfalls in Paare von je zweien ordnen, aber so dass das Produkt der Zahlen jedes Paares $\equiv -1 \pmod{m}$ ist; denn wenn a eine Wurzel der Congruenz $x^2 \equiv 1 \pmod{m}$ ist, so ist es auch $-a$, und es ist

$$a \cdot (-a) = -a^2 \equiv -1 \pmod{m}.$$

Das Produkt aller in Rede stehenden Zahlen ist daher

$$\equiv -1 \pmod{m},$$

wenn die Congruenz $x^2 \equiv 1 \pmod{m}$ nur zwei Wurzeln besitzt, d. i. wenn m eine Potenz einer ungeraden Primzahl, oder das Doppelte einer solchen Potenz, oder gleich 4 ist. In allen andern Fällen hat die Congruenz $x^2 \equiv 1 \pmod{m}$ nach dem Früheren 2^k Wurzeln, wo $k \geq 2$ ist, und dann ist das Produkt aller Zahlen, die prim zu m und nicht grösser als m sind, $\equiv +1 \pmod{m}$.

Anmerkung. Der erste Theil des Satzes ergiebt sich durch Anwendung der Indices leicht auf folgende Weise:

Es bezeichne g eine primitive Wurzel von m, so stellen die Potenzen

$$g,\ g^2,\ g^3,\ \ldots,\ g^{\varphi(m)}$$

die Zahlen dar, die prim zu m und nicht grösser als m sind. Das Produkt dieser Zahlen ist

$$g^{1+2+\cdots+\varphi(m)} = g^{[1+\varphi(m)]\frac{1}{2}\varphi(m)} = g^{\frac{1}{2}\varphi(m)} \cdot g^{\frac{1}{2}\varphi(m)\varphi(m)}.$$

$g^{\frac{1}{2}\varphi(m)}$ ist aber $\equiv -1$, $g^{\varphi(m)} \equiv +1 \pmod{m}$, und somit giebt das betrachtete Produkt den Rest -1.

§ 82. Ueber die Moduln, für welche eine gegebene Zahl Rest ist. — Nachdem wir im Vorhergehenden untersucht haben, welche Zahlen Reste eines gegebenen Moduls sind, haben wir umgekehrt die schwierigere Frage zu behandeln, für welche Moduln eine gegebene Zahl Rest ist. Wir können uns dabei auf Primzahlmoduln beschränken, da der § 80 uns gelehrt hat, dass eine Zahl nur dann Rest eines zusammengesetzten Moduls ist, wenn sie Rest jedes einzelnen seiner Primfactoren ist. Da ferner der Modul $2^\varkappa$ in § 79 seine Erledigung gefunden hat, so bleiben nur die ungeraden Primzahlen zu ermitteln, für welche die gegebene Zahl Rest ist.

Eine weitere Vereinfachung erfährt die Aufgabe noch durch den § 78, in welchem gezeigt ist, dass eine zusammengesetzte Zahl Rest oder Nichtrest einer ungeraden Primzahl ist, je nachdem sie eine gerade oder ungerade Anzahl von Factoren enthält, die Nichtreste dieser Primzahl sind. Unsere Aufgabe reducirt sich also auf die Beantwortung der Frage:

Für welche ungeraden Primzahlen als Moduln ist jede der drei Zahlen -1, $+2$, $+q$, wo q eine ungerade Primzahl bezeichnet, quadratischer Rest?

§ 83. Moduln, für welche -1 Rest ist. —

Lehrsatz. Die Zahl -1 ist Rest aller Primzahlen von der Form $4n+1$, Nichtrest aller Primzahlen von der Form $4n+3$.

1. Beweis. Nach § 77 ist -1 Rest von p, wenn

$$(-1)^{\frac{p-1}{2}} = +1$$

ist; dies erfordert, dass $\frac{p-1}{2}$ eine gerade Zahl sei, etwa $\frac{p-1}{2} = 2n$; dann ist $p = 4n+1$.

Nach demselben Paragraphen ist -1 Nichtrest von p, wenn $(-1)^{\frac{p-1}{2}} = -1$ ist; dies erfordert, dass $\frac{p-1}{2}$ ungerade, etwa $\frac{p-1}{2} = 2n+1$ sei; dann ist aber $p = 4n+3$.

Wenn umgekehrt $p = 4n+1$ ist, so ergiebt sich

$$(-1)^{\frac{p-1}{2}} = +1,$$

und wenn $p = 4n+3$ ist, so folgt

$$(-1)^{\frac{p-1}{2}} = -1;$$

somit ist -1 für jede Primzahl $p = 4n+1$ Rest, für jede Primzahl $p = 4n+3$ Nichtrest.

2. Beweis. Nach § 75 befinden sich unter den Zahlen $1, 2, 3, \ldots, p-1$ ebenso viele Reste wie Nichtreste, nämlich $\frac{p-1}{2}$ Zahlen jeder der beiden Arten; daher wird das Produkt aller Zahlen $1, 2, 3, \ldots, p-1$ nach § 78 ein Rest oder ein Nichtrest sein, je nachdem $\frac{p-1}{2}$ gerade oder ungerade ist. Da nun dieses Produkt nach dem Wilson'schen Satze

$$\equiv -1 \pmod{p}$$

ist, so ist auch -1 Rest oder Nichtrest von p, je nachdem $\frac{p-1}{2}$ gerade oder ungerade ist, d. h. je nachdem p die Form $4n+1$ oder $4n+3$ hat.

Zusatz. Jede Primzahl von der Form $4n+1$ ist die Summe zweier Quadrate, welche prim zu einander sind.

Beweis. Wenn $p = 4n+1$ ist, so ist -1 Rest von p, d. h. es lässt sich eine Zahl a von der Beschaffenheit ermitteln, dass $a^2 \equiv -1 \pmod{p}$, also a^2+1 durch p theilbar sei. Dann muss aber nach § 37 p selbst die Summe zweier Quadrate sein, und diese sind prim zu einander, weil ein beiden gemeinschaftlicher Divisor auch in p ohne Rest aufgehen müsste.

Auf welche Weise die Zerlegung von p in zwei Quadrate ausgeführt werden kann, ist schon § 37 gezeigt worden; auch werden wir später auf den Gegenstand nochmals zurückkommen.

§ 84. Moduln, für welche $+2$ Rest ist. — Die Zahl 2 hat, wie ein Durchblicken der Index-Tabelle ergiebt, einen geraden Index für die Moduln 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Für diese Primzahlen, die von den Formen $8n+1$, $8n+7$ sind, ist also 2 Rest.

Der Index von 2 ist ungerade für die Moduln 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83. Für diese Primzahlen, die von den Formen $8n+3$, $8n+5$ sind, ist also 2 Nichtrest.

Lehrsatz. Die Zahl 2 ist Rest aller Primzahlen der Formen $8n+1$, $8n+7$, Nichtrest dagegen aller Primzahlen der Formen $8n+3$, $8n+5$.

Beweis. I. Wir beweisen zunächst, dass 2 Nichtrest aller Primzahlen $8n+3$, $8n+5$ oder, was dasselbe ist, Nichtrest aller Primzahlen $8n \pm 3$ ist. Jedenfalls ist der Satz für die Primzahlen unter 100 richtig; wäre derselbe nun nicht allgemein gültig, so müsste es Primzahlen der Formen $8n \pm 3$ geben, für welche 2 Rest wäre. Die kleinste dieser Zahlen sei t, d. h. es sei t die kleinste Primzahl einer der beiden

Formen $8n \pm 3$, für welche als Modul die Congruenz $x^2 \equiv 2$ möglich ist. Die Congruenz hat nach § 75 zwei entgegengesetzt gleiche Wurzeln, die wir mit $+a$ und $-a \equiv t - a$ bezeichnen wollen, und von denen jede $< t$ ist. Je nachdem nun a gerade oder ungerade ist, wird $t - a$ ungerade oder gerade sein. Wir dürfen daher eine der Wurzeln als ungerade voraussetzen. Es sei a ungerade und $< t$. Da nun a Wurzel der Congruenz

$$x^2 \equiv 2 \pmod{t}$$

sein soll, so können wir $a^2 = 2 + tu$, also $tu = a^2 - 2$ setzen, wo u eine ganze Zahl bezeichnet. Dies giebt $tu < a^2$. Es ist aber $a < t$, also auch $a^2 < t^2$; umsomehr wird $tu < t^2$, also $u < t$ sein. Was ferner die Form von u betrifft, so ist a^2 von der Form $8n + 1$ (das Quadrat jeder ungeraden Zahl hat diese Form), also $tu = a^2 - 2$ von der Form $8n - 1$, und da t von der Form $8n \pm 3$ ist, so muss u die Form $8n \mp 3$ haben.

Aus der Gleichung $a^2 = 2 + tu$ folgt aber, dass

$$a^2 \equiv 2 \pmod{u}$$

sein muss. Es wird also die Congruenz $x^2 \equiv 2$ auch für einen Modul u bestehen, der $< t$ und gleichfalls von einer der beiden Formen $8n \pm 3$ ist.

Dies widerspricht, wenn u eine Primzahl ist, der Voraussetzung, nach welcher t die kleinste Primzahl sein soll, für welche 2 Rest ist. Ist dagegen u eine zusammengesetzte Zahl, so muss diese wenigstens einen Primzahlfactor v einer der Formen $8n \pm 3$ enthalten, da Factoren der Formen $8n \pm 1$ niemals ein Produkt einer der Formen $8n \pm 3$ liefern können. Da dann 2 auch Rest von v sein müsste und v gleichfalls $< t$ ist, so würde sich derselbe Widerspruch ergeben.

2 ist also Nichtrest der Primzahlen $8n + 3$ und $8n + 5$.

II. Wir wollen jetzt beweisen, dass 2 Rest aller Primzahlen $8n + 7$ ist. Da -1 nach § 83 Nichtrest dieser Zahlen ist, so brauchen wir nur darzuthun, dass -2 Nichtrest aller Primzahlen $8n + 7$ sei. Statt dessen beweisen wir, dass -2 Nichtrest aller Primzahlen der beiden Formen $8n + 5$, $8n + 7$ ist (obwohl wir dies für die Primzahlen $8n + 5$, für welche -1 Rest ist, schon nach dem Vorhergehenden wissen).

Die Zahl 5 hat die Reste 1, 4, die Nichtreste 2, 3 — 2. Also ist — 2 Nichtrest von 5. Ebenso ist — 2 Nichtrest von 7. Wäre nun der Satz nicht allgemein gültig, d. h. gäbe es Primzahlen der Formen $8n+5$, $8n+7$, für welche -2 Rest wäre, so könnten wir wieder die kleinste derselben, t, wählen und erhielten, wenn wir die ungerade Wurzel der Congruenz

$$x^2 \equiv -2 \pmod{t}$$

mit a bezeichneten,

$$a^2 \equiv -2 \pmod{t}, \quad \text{also} \quad -2 = a^2 - tu,$$

und hieraus würde wieder, da $a < t$ ist, $u < t$ folgen. Weiter würde sich ergeben, dass u von der Form $8n+5$ oder $8n+7$ sein müsste, je nachdem t die Form $8n+7$ oder $8n+5$ hätte. Endlich würde aus der Annahme $-2 = a^2 - tu$ noch

$$-2 \equiv a^2 \pmod{u}$$

folgen, es müsste also -2 auch Rest von u sein. Wenn u eine Primzahl ist, so widerspricht dies der Voraussetzung, nach welcher t die kleinste Primzahl der Formen $8n+5$, $8n+7$ sein soll, für welche -2 Rest ist. Ist aber u eine zusammengesetzte Zahl, so muss diese wenigstens einen Primzahlfactor v einer der Formen $8n+5$, $8n+7$ enthalten, und dann müsste -2 auch Rest dieses noch kleineren Factors sein, was ebenfalls der Voraussetzung widerspricht. Es ist also -2 Nichtrest aller Primzahlen $8n+5$ und $8n+7$, folglich $+2$ Rest aller Primzahlen $8n+7$.

III. Endlich haben wir noch zu beweisen, dass 2 Rest jeder Primzahl $8n+1$ ist. Es sei g eine primitive Wurzel von $8n+1$, so ist nach dem Fermat'schen Satze $(g^{4n})^2 \equiv +1$ und, weil g^{4n} nicht $\equiv +1$ sein kann, da g sonst zum Exponenten $4n$ gehören würde, $g^{4n} \equiv -1$ oder

$$g^{4n} + 1 \equiv 0 \pmod{\overline{8n+1}}.$$

Nun ist

$$(g^{2n}+1)^2 = g^{4n} + 2g^{2n} + 1,$$

also mit Rücksicht auf die vorhergehende Congruenz

$$(g^{2n}+1)^2 \equiv 2g^{2n} \pmod{\overline{8n+1}}.$$

Daraus geht hervor, dass $2g^{2n}$ Rest von $8n+1$ ist, und da g^{2n} ein durch den Modul nicht theilbares Quadrat ist, so ist auch 2 Rest von $8n+1$.

Zusatz. Die Zahl -2 ist Rest jeder Primzahl der Formen $8n+1$, $8n+3$, Nichtrest dagegen jeder Primzahl der Formen $8n+5$ und $8n+7$.

Der Beweis ergiebt sich sofort, indem man

$$-2 = (-1) \cdot 2$$

annimmt und die in § 83 und 84 gewonnenen Resultate mit Rücksicht auf § 78 verbindet.

§ 85. Anderes Mittel, zu entscheiden, ob eine gegebene Zahl Rest oder Nichtrest einer Primzahl sei. — Anwendungen. — **Lehrsatz.** Bezeichnet a eine Zahl, die prim zu der ungeraden Primzahl p ist, und bildet man die kleinsten positiven Reste der Produkte

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a,$$

so wird ein Theil derselben $< \frac{1}{2}p$, ein Theil $> \frac{1}{2}p$ sein. Wird die Anzahl der Reste, die $> \frac{1}{2}p$ sind, mit μ bezeichnet, so ist a Rest oder Nichtrest von p, je nachdem μ gerade oder ungerade ist.

Beweis. Werden diejenigen Reste der obigen Produkte, welche $< \frac{1}{2}p$ sind, mit $r_1, r_2, r_3, \ldots$, die übrigen μ, die $> \frac{1}{2}p$ sind, mit $R_1, R_2, R_3, \ldots R_\mu$ bezeichnet, so sind die Ergänzungen der letzteren zum Modul, nämlich $p - R_1$, $p - R_2$, $p - R_3, \ldots, p - R_\mu$ gleichfalls $< \frac{1}{2}p$ und sowohl unter einander, als auch von den Resten $r_1, r_2, r_3, \ldots$ verschieden; denn die Congruenz $p - R_\varkappa \equiv p - R_\lambda$ würde die folgende nach sich ziehen: $R_\varkappa \equiv R_\lambda \pmod{p}$, und aus der Annahme $p - R_\varkappa \equiv r_\lambda$ würde $R_\varkappa + r_\lambda \equiv 0 \pmod{p}$ folgen, und beides ist offenbar unmöglich. Daher werden die Zahlen

$$r_1,\ r_2,\ r_3,\ \ldots,\ p - R_1,\ p - R_2,\ \ldots,\ p - R_\mu$$

in irgend einer Reihenfolge mit den Zahlen $1, 2, 3, \ldots, \frac{p-1}{2}$ übereinstimmen, und das Produkt der ersteren muss gleich dem Produkt der letzteren sein. Wir erhalten also

$$r_1 \cdot r_2 \cdot r_3 \ldots (p - R_1)(p - R_2) \ldots (p - R_\mu) = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$$

und durch Weglassung der Vielfachen von p

$$(-1)^\mu r_1 r_2 r_3 \ldots R_1 R_2 \ldots R_\mu \equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}.$$

Andererseits ergiebt sich, wenn wir das Produkt der betrachteten Zahlen $a, 2a, \ldots, \frac{p-1}{2}a$ dem Produkt ihrer Reste congruent setzen

$$1\,.\,2\,.\,3\cdots\frac{p-1}{2}\cdot a^{\frac{p-1}{2}} \equiv r_1\,r_2\,r_3\ldots R_1\,R_2\ldots R_\mu \pmod{p},$$

und mit Rücksicht hierauf geht die vorhergehende Congruenz über in

$$(-1)^\mu\,a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

oder in

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}.$$

$a^{\frac{p-1}{2}}$ ist also $\equiv +1$ oder $\equiv -1$, d. h. a ist Rest oder Nichtrest von p, je nachdem μ gerade oder ungerade ist.

Anwendungen. I. Um zu ermitteln, von welchen Primzahlen 2 quadratischer Rest ist, haben wir die Reste der Produkte $2, 4, 6, \ldots, p-1$ zu bilden und zu sehen, wie viele derselben kleiner und wie viele $> \frac{1}{2}p$ sind. Wir wollen die letzteren von den ersteren durch einen Vertikalstrich trennen. Jene Produkte lassen sich dann, je nachdem p eine der vier Formen $8n+1$, $8n+3$, $8n+5$, $8n+7$ hat, in folgender Weise schreiben:

$2, 4, 6, \ldots, 4n \mid 4n+2, \ldots, 8n$
$2, 4, 6, \ldots, 4n \mid 4n+2, \ldots, 8n, 8n+2$
$2, 4, 6, \ldots, 4n+2 \mid 4n+4, \ldots, 8n, 8n+2, 8n+4$
$2, 4, 6, \ldots, 4n+2 \mid 4n+4, \ldots, 8n+4, 8n+6.$

Im ersten Falle sind also $\frac{8n-4n}{2} = 2n$,

im zweiten

$$\frac{(8n+2)-4n}{2} = 2n+1,$$

im dritten

$$\frac{(8n+4)-(4n+2)}{2} = 2n+1,$$

endlich im vierten

$$\frac{(8n+6)-(4n+2)}{2} = 2n+2$$

Zahlen $> \frac{p}{2}$, d. h. 2 ist Rest der Primzahlen $8n+1$, $8n+7$, Nichtrest der Primzahlen $8n+3$, $8n+5$.

II. Um zu ermitteln, von welchen Primzahlen 3 quadratischer Rest ist, bilden wir die Reste der Produkte

$$3,\ 6,\ 9,\ \ldots,\ \frac{3(p-1)}{2}$$

und ermitteln, wie viele dieser Reste $> \frac{p}{2}$ sind. Nun kann p eine der vier Formen

$$12n+1,\quad 12n+5,\quad 12n+7,\quad 12n+11$$

haben. Wenn e r s t e n s $p = 12n+1$ ist, so ist

$$\frac{3(p-1)}{2} = 18n$$

die letzte zu betrachtende Zahl. Nun sind zunächst die Produkte $3, 6, 9, \ldots, 6n$ sämmtlich $< \frac{1}{2}p$, kommen also nicht in Betracht; dann folgen die Produkte $6n+3$, $6n+6$, $\ldots$, $12n$, die sämmtlich $> \frac{1}{2}p$ sind; hieran schliessen sich endlich die Produkte $12n+3$, $12n+6$, $\ldots$, $18n$, die sämmtlich $> p$ sind; diese müssen durch ihre kleinsten positiven Reste $2, 5, \ldots, 6n-1$ ersetzt werden, und da diese letzteren sämmtlich $< \frac{p}{2}$ sind, so kommen auch sie nicht in Betracht. Es sind also nur die Reste

$$6n+3,\ \ldots,\ 12n$$

grösser als $\frac{p}{2}$, und da ihre Anzahl $\frac{12n-6n}{3} = 2n$, also gerade ist, so ist 3 Rest jeder Primzahl $12n+1$.

Ebenso zerfallen für jede der drei anderen Formen von p die betrachteten Produkte in je drei Gruppen, von denen nur die mittlere die Reste enthält, die grösser als $\frac{p}{2}$ sind. Wir wollen in jedem Falle diese mittlere Gruppe durch Verticalstriche von den anderen trennen. Es sind danach z w e i t e n s für $p = 12n+5$ die Reste der in Rede stehenden Zahlen

$$3,\ 6,\ 9,\ \ldots,\ 6n \mid 6n+3,\ \ldots,\ 12n+3 \mid$$
$$12n+6 \equiv 1, 4,\ \ldots,\ 18n+6 \equiv 6n+1;$$

die mittlere Gruppe enthält

$$\frac{(12n+3)-6n}{3} = 2n+1$$

Glieder; da $2n+1$ eine ungerade Zahl ist, so ist 3 Nichtrest jeder Primzahl $12n+5$. Drittens sind für

$$p = 12n + 7$$

die Reste der in Rede stehenden Zahlen

$$3, 6, 9, \ldots, 6n+3 \mid 6n+6, \ldots, 12n+6 \mid$$
$$12n+9 \equiv 2, 5, \ldots, 18n+9 \equiv 6n+2,$$

und da die mittlere Gruppe

$$\frac{(12n+6)-(6n+3)}{3} = 2n+1,$$

also eine ungerade Anzahl Glieder enthält, so ist 3 Nichtrest jeder Primzahl $12n+7$.

Wenn endlich p die Form $12n+11$ hat, so sind die Reste der betrachteten Produkte

$$3, 6, \ldots, 6n+3 \mid 6n+6, \ldots, 12n+9 \mid$$
$$12n+12 \equiv 1, 4, \ldots, 18n+15 \equiv 6n+4,$$

und da die mittlere Gruppe

$$\frac{(12n+9)-(6n+3)}{3} = 2n+2,$$

also eine gerade Anzahl Glieder hat, so ist 3 Rest jeder Primzahl $12n+11$.

Anmerkung. Da die Zahlen der beiden Formen $12n+1$, $12n+5$ von der Form $4n+1$, diejenigen der beiden Formen $12n+7$, $12n+11$ von der Form $4n+3$ sind, so ergiebt sich durch Verbindung der eben erhaltenen Resultate mit dem Ergebniss des § 83 der Satz:

Die Zahl -3 ist Rest aller Primzahlen der Formen $12n+1$, $12n+7$, Nichtrest aller Primzahlen der Formen $12n+5$, $12n+11$.

§ 86. Der Reciprocitäts-Satz. — Wir haben jetzt noch zu untersuchen, von welchen ungeraden Primzahlen p eine gegebene ungerade Primzahl q Rest ist. Diese Frage beantwortet einer der interessantesten Sätze der Zahlentheorie, der Reciprocitäts-Satz, der sich folgendermassen aussprechen lässt:

Wenn p und q zwei positive ungerade Primzahlen sind, von denen wenigstens eine die Form $4n+1$ hat, so ist q Rest oder Nichtrest von p, je nachdem p Rest

oder Nichtrest von q ist. Hat aber jede der beiden Zahlen p, q die Form $4n + 3$, so ist q Rest oder Nichtrest von p, je nachdem p Nichtrest oder Rest von q ist.

Dieser Satz ist von Legendre durch Induction gefunden worden (Théorie des nombres, II, § 6); erst Gauss gelang es, ihn zu beweisen. Gauss hat sich mit dem wichtigen Satze lange beschäftigt und nach einander sechs Beweise desselben gegeben, denen später noch andere Beweise von Eisenstein, Liouville u. A. gefolgt sind. Bei Anwendung des Legendre'schen Symbols lässt sich der Satz durch die Formel

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ausdrücken; denn wenn eine der beiden Zahlen p, q von der Form $4n + 1$ ist, so hat die rechte Seite der Formel den Werth $+1$; folglich muss jedes der Symbole $\left(\frac{p}{q}\right)$, $\left(\frac{q}{p}\right)$ entweder den Werth $+1$ oder den Werth -1 haben. Hat aber jede der Zahlen p, q die Form $4n + 3$, so ist die rechte Seite der Formel gleich -1, und somit hat von den Symbolen $\left(\frac{p}{q}\right)$, $\left(\frac{q}{p}\right)$ das eine den Werth $+1$, das andere den Werth -1.

Wir geben im Folgenden zunächst den fünften der von Gauss veröffentlichten Beweise (Bd. II, p. 51).

§ 87. Beweis des Reciprocitäts-Satzes. Um zu sehen, ob p Rest oder Nichtrest von q sei, hat man nach § 85 die Produkte

$$p,\ 2p,\ 3p,\ \ldots,\ \frac{q-1}{2}\,p \tag{1}$$

zu nehmen, ihre kleinsten Reste für den Modul q zu bilden und zu zählen, wie viele dieser Reste grösser als $\frac{q}{2}$ sind; die Anzahl dieser letzteren sei n.

Um zu sehen, ob q Rest oder Nichtrest von p sei, hat man ebenso die Produkte

$$q,\ 2q,\ 3q,\ \ldots,\ \frac{p-1}{2}\,q \tag{2}$$

zu untersuchen; von den Resten derselben seien ν grösser als $\frac{p}{2}$.

Es ist dann p Rest oder Nichtrest von q, je nachdem n gerade oder ungerade ist, und ebenso q Rest oder Nichtrest von p, je nachdem ν gerade oder ungerade ist.

Wir betrachten nun statt der Reihen (1) und (2) die Reihe der Zahlen

$$(3) \qquad 1, 2, 3, \ldots, \tfrac{1}{2}(pq-1),$$

welche, da ihr letztes Glied sowohl grösser wie das letzte Glied von (1), als auch grösser wie das letzte Glied von (2) ist, die Zahlen der Reihen (1) und (2) in sich schliesst.

Unter den Zahlen der Reihe (3) sind also zunächst alle in (1) enthaltenen Vielfachen von p. Die kleinsten positiven Reste dieser Vielfachen von p, für den Modul q genommen, sind entweder $> \frac{q}{2}$ oder $< \frac{q}{2}$, und da die Anzahl der ersteren der Voraussetzung nach gleich n ist, so muss die der letzteren $\frac{q-1}{2} - n$ sein.

Ferner enthält die Reihe (3) alle in (2) befindlichen Vielfachen von q; die Reste derselben, für den Modul p genommen, sind entweder $> \frac{1}{2}p$ oder $< \frac{1}{2}p$, und da die Anzahl der ersteren der Voraussetzung nach gleich ν ist, so wird die der letzteren $\frac{p-1}{2} - \nu$ sein.

Was endlich die übrigen Zahlen der Reihe (3) betrifft, so befinden sich darunter

solche, deren Reste für den Modul p kleiner als $\frac{1}{2}p$ und zugleich für den Modul q kleiner als $\frac{1}{2}q$ sind; die Anzahl dieser Zahlen sei α;

solche, deren Reste für den Modul p kleiner als $\frac{1}{2}p$ und zugleich für den Modul q grösser als $\frac{1}{2}q$ sind; die Anzahl derselben sei β;

solche, deren Reste für den Modul p grösser als $\frac{1}{2}p$ und zugleich für den Modul q kleiner als $\frac{1}{2}q$ sind; die Anzahl derselben sei γ; endlich

solche, deren Reste für den Modul p grösser als $\frac{1}{2}p$ und zugleich für den Modul q grösser als $\frac{1}{2}q$ sind; die Anzahl derselben sei δ.

In derselben Weise kann man die Zahlen der an (3) sich anschliessenden Reihe

(4) $\frac{1}{2}(pq+1), \ldots, pq-3, pq-2, pq-1,$

welche ebenso viele Glieder wie (3) enthält, nach den Resten, welche sie beziehungsweise für die Moduln p, q geben, in Gruppen zerlegen. Da nun allgemein

$$pq - a \equiv -a \equiv p - a \pmod{p}$$

und ebenso

$$pq - a \equiv -a \equiv q - a \pmod{q}$$

ist, und da

$$p - a \gtrless \tfrac{1}{2}p, \text{ je nachdem } a \lessgtr \tfrac{1}{2}p,$$

$$q - a \gtrless \tfrac{1}{2}q, \text{ je nachdem } a \lessgtr \tfrac{1}{2}q$$

ist, so wird für jede Zahl a der Reihe (3), deren Rest für den Modul p grösser oder kleiner als $\frac{1}{2}p$ ist, die Reihe (4) eine Zahl $p - a$ enthalten, deren Rest beziehungsweise kleiner oder grösser als $\frac{1}{2}p$ ist, und dasselbe gilt hinsichtlich des Moduls q.

Die Reihe (4) enthält also

α Zahlen, deren Reste für den Modul p grösser als $\frac{1}{2}p$ und zugleich für den Modul q grösser als $\frac{1}{2}q$ sind;

β Zahlen, deren Reste für den Modul p grösser als $\frac{1}{2}p$ und zugleich für den Modul q kleiner als $\frac{1}{2}q$ sind;

γ Zahlen, deren Reste für den Modul p kleiner als $\frac{1}{2}p$ und zugleich für den Modul q grösser als $\frac{1}{2}q$ sind;

δ Zahlen, deren Reste für den Modul p kleiner als $\frac{1}{2}p$ und zugleich für den Modul q kleiner als $\frac{1}{2}q$ sind.

Es sind also in den Reihen (3) und (4) zusammen, d. h. unter den Zahlen von 1 bis $pq - 1$ $\alpha + \delta$ Zahlen vorhanden, deren Reste für den Modul p kleiner als $\frac{1}{2}p$, d. h. eine der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(p-1)$ sind, und welche gleichzeitig für den Modul q eine der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(q-1)$ zum Rest haben. Da nun die Anzahl der Zahlen, die diesen beiden Bedingungen genügen, offenbar $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ ist, so erhalten wir die Gleichung

$$\text{(I)} \qquad \alpha + \delta = \tfrac{1}{4}(p-1)(q-1).$$

Unter den Zahlen von 1 bis $pq - 1$ befinden sich ebenso $\beta + \gamma$ Zahlen, welche für den Modul p einen Rest $> \frac{1}{2}p$ geben, also eine der $\frac{1}{2}(p-1)$ Zahlen $\frac{1}{2}(p+1), \ldots, (p-1)$ zum Rest haben, und welche gleichzeitig für den Modul q eine der $\frac{1}{2}(q-1)$ Zahlen $\frac{1}{2}(q+1), \ldots, q-1$ zum Rest

haben. Da die Anzahl dieser Zahlen $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ sein muss, so ist

(II) $$\beta + \gamma = \tfrac{1}{4}(p-1)(q-1).$$

Fassen wir weiter die Zahlen der Reihe (3) ins Auge, deren Reste für den Modul q grösser als $\frac{1}{2}q$ sind, so sind es zunächst n Vielfache von p, welche diese Eigenschaft besitzen, dann aber, wie wir gesehen haben, noch $\beta + \delta$, also im Ganzen $n + \beta + \delta$ Zahlen.

Andererseits sind dies folgende Zahlen (die kleinste derselben, d. i. $\frac{1}{2}(q+1)$, soll der Kürze wegen mit a bezeichnet werden):

$$\begin{array}{l} a,\ a+1,\ a+2, \ldots, q-1, \\ a+q,\ a+q+1,\ a+q+2, \ldots, q+q-1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a+\frac{p-3}{2}q,\ \ a+\frac{p-3}{2}q+1, \ldots, \frac{p-3}{2}q+q-1. \end{array}$$

Da jede Horizontalreihe aus $q - a = \frac{1}{2}(q-1)$ Gliedern besteht, und da $\frac{p-3}{2} + 1 = \frac{1}{2}(p-1)$ solcher Reihen vorhanden sind, so ist die Anzahl dieser Zahlen

$$\tfrac{1}{2}(q-1) \cdot \tfrac{1}{2}(p-1),$$

also

(III) $$n + \beta + \delta = \tfrac{1}{4}(p-1)(q-1).$$

Ebenso ergiebt sich durch doppelte Zählung der Zahlen von (3), welche für den Modul p Reste haben, die $> \frac{1}{2}p$ sind,

(IV) $$\nu + \gamma + \delta = \tfrac{1}{4}(p-1)(q-1).$$

Durch Addition der drei letzten Gleichungen erhält man

(V) $$2\beta + 2\gamma + 2\delta + n + \nu = \tfrac{3}{4}(p-1)(q-1),$$

und daraus entnehmen wir Folgendes: Wenn eine der Zahlen p, q die Form $4n + 1$ hat, so ist die rechte Seite von (V) eine gerade Zahl, also muss auch die linke und somit $n + \nu$ gerade sein; in diesem Falle sind also n, ν beide gerade oder beide ungerade, oder q ist Rest von p, wenn p Rest von q ist, und q ist Nichtrest von p, wenn p Nichtrest von q ist.

Hat dagegen jede der Zahlen p, q die Form $4n + 3$, so ist die rechte Seite von (V) eine ungerade Zahl; daher muss auch die linke Seite und somit $n + \nu$ ungerade sein; das ist

aber nur möglich, wenn eine der Zahlen u, v gerade, die andere ungerade ist; in diesem Falle ist also q Nichtrest von p, wenn p Rest von q ist, und q Rest von p, wenn p Nichtrest von q ist.

§ 88. Eisenstein's geometrischer Beweis des Reciprocitätssatzes (Crelle, Journal, Bd. 28). — Es sei p eine positive ungerade Primzahl, a der Complex der Zahlen $2, 4, 6, \ldots, p-1$ und q eine beliebige durch p nicht theilbare ganze Zahl. Wir bilden die für den Modul p offenbar incongruenten Produkte

$$2q, 4q, 6q, \ldots, (p-1)q$$

und nehmen deren kleinste positive Reste für den Modul p.

Diese Reste sind theils gerade, theils ungerade Zahlen; die ersteren gehören dem Complex a an, die letzteren nicht. Ein gerader Rest r bleibt unverändert, wenn man ihm den Factor $(-1)^r$ zutheilt; ein ungerader Rest r dagegen wird durch Zutheilung dieses Factors in eine negative ungerade Zahl verwandelt, also congruent einer geraden Zahl, die ebenfalls dem Complex a angehört. Der Complex aller Zahlen $(-1)^r r$ wird also zusammenfallen mit dem Complex a, und daher ist das Produkt aller Zahlen $(-1)^r r$ für den Modul p congruent dem Produkt aller Zahlen a, in Zeichen

$$(-1)^{\Sigma r}\, \Pi(r) \equiv \Pi(a) \pmod{p}.$$

Andererseits ist das Produkt aller Produkte qa

$$\Pi qa = 2q \cdot 4q \cdot 6q \ldots (p-1)\, q = q^{\frac{p-1}{2}} \cdot \Pi a,$$

also, da

$$qa \equiv r \pmod{p}$$

sein soll,

$$q^{\frac{p-1}{2}}\, \Pi a \equiv \Pi r \pmod{p}.$$

Aus den beiden erhaltenen Congruenzen folgt

$$q^{\frac{p-1}{2}} \cdot (-1)^{\Sigma r} \equiv 1 \pmod{p}$$

oder

$$q^{\frac{p-1}{2}} \equiv (-1)^{\Sigma r} \pmod{p},$$

d. i. bei Anwendung des Legendre'schen Symbols

$$\left(\frac{q}{p}\right) = (-1)^{\Sigma r}.$$

Bezeichnet nun $E\left(\frac{qa}{p}\right)$ die grösste in dem Bruche $\frac{qa}{p}$ enthaltene ganze Zahl, so folgt aus

$$qa = pE\left(\frac{qa}{p}\right) + r,$$

dass

$$\Sigma qa = p\Sigma E\left(\frac{qa}{p}\right) + \Sigma r$$

ist. Da a gerade ist, so ist $\Sigma qa \equiv 0 \pmod{2}$; ferner ist

$$p \equiv 1 \pmod{2},$$

also

$$\Sigma r \equiv -\Sigma E\left(\frac{qa}{p}\right) \equiv \Sigma E\left(\frac{qa}{p}\right) \pmod{2}$$

und

$$\left(\frac{q}{p}\right) = (-1)^{\Sigma E\left(\frac{qa}{p}\right)}.$$

Wenn $q = 2$ ist, so liefert diese Formel durch eine Betrachtung, welche der in § 85 angestellten ganz ähnlich ist, direkt den Werth des Symbols $\left(\frac{2}{p}\right)$.

Ist dagegen q ungerade, also $q - 1$ gerade, so ist

$$\Sigma E\left(\frac{qa}{p}\right) = E\left(\frac{2q}{p}\right) + E\left(\frac{4q}{p}\right) + \cdots + E\left(\frac{\frac{1}{2}(p-1)q}{p}\right) + \cdots + E\left(\frac{(p-1)q}{p}\right).$$

Setzt man nun

$$\frac{nq}{p} = E\left(\frac{nq}{p}\right) + \varrho,$$

wo ϱ ein positiver echter Bruch ist, und subtrahirt diese Gleichung von $q = q$, so erhält man

$$q - \frac{nq}{p}, \text{ d. i. } \frac{(p-n)q}{p} = (q-1) - E\left(\frac{nq}{p}\right) + (1-\varrho);$$

es ist also allgemein

$$E\left(\frac{(p-n)q}{p}\right) = (q-1) - E\left(\frac{nq}{p}\right)$$

oder, wenn rechts die gerade Zahl $2E\left(\frac{nq}{p}\right) - (q-1)$ addirt wird,

$$E\left(\frac{(p-n)q}{p}\right) \equiv E\left(\frac{nq}{q}\right) \pmod{2}.$$

Danach ist also

$$\left.\begin{array}{l} E\left(\frac{(p-1)q}{p}\right) \equiv E\left(\frac{q}{p}\right) \\ E\left(\frac{(p-3)q}{p}\right) \equiv E\left(\frac{3q}{p}\right) \\ \ldots\ldots\ldots\ldots \end{array}\right\} \pmod{2},$$

so dass wir

$$\Sigma E\left(\frac{qa}{p}\right) \equiv E\left(\frac{q}{p}\right) + E\left(\frac{2q}{p}\right) + E\left(\frac{3q}{p}\right) + \cdots + E\left(\frac{\frac{1}{2}(p-1)q}{p}\right) \pmod{2}$$

erhalten, und wenn diese Zahl mit μ bezeichnet wird, so ist

$$\left(\frac{q}{p}\right) = (-1)^{\mu}.$$

Wir denken uns jetzt in der Ebene ein rechtwinkliges Coordinaten-System gezogen und die ganze Ebene durch Parallele zu den Axen in den Abständen $= 1$ in lauter Quadrate getheilt. Alle Ecken der Quadrate, die nicht in den Coordinaten-Axen liegen, sollen **Gitterpunkte** heissen.

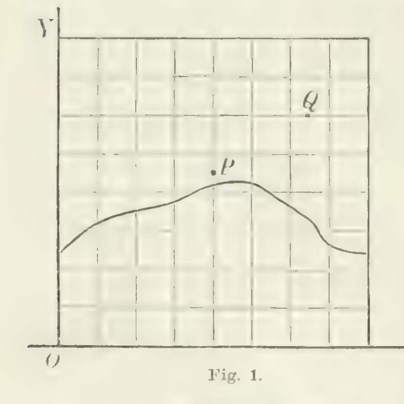


Fig. 1.

Nimmt man auf einer Parallele zur y-Axe einen Punkt y an (in der Figur P), so bezeichnet $E(y)$ die Anzahl der Gitterpunkte, welche zwischen diesem Punkte und der x-Axe liegen (in der Figur 4). Wird ebenso auf einer Parallelen zur x-Axe ein Punkt x angenommen (in der Figur Q), so wird $E(x)$ ausdrücken, wie viele Gitterpunkte auf dieser Parallelen zwischen dem Punkte und der y-Axe liegen (in der Figur 6). Zeichnet man also in der Ebene eine Curve, deren Gleichung $y = \varphi(x)$ ist, so bezeichnen $E\varphi(1)$, $E\varphi(2)$, $E\varphi(3)$, ... beziehungsweise die Anzahl der Gitterpunkte, welche auf der ersten, zweiten, dritten, ... Parallele zur y-Axe zwischen der Curve und der x-Axe liegen, also

$$E\varphi(1) + E\varphi(2) + E\varphi(3) + \cdots$$

die Anzahl aller Gitterpunkte zwischen der Curve und der x-Axe. Dabei sind die Gitterpunkte, die etwa zufällig auf der Curve selbst liegen, mitgerechnet worden.

Es sei nun AB diejenige gerade Linie, deren Gleichung $y = \frac{q}{p}\, x$ ist, wo p, q als positive ungerade Primzahlen vorausgesetzt werden. $AD = FB$ sei $= p$, $AF = BD = q$,

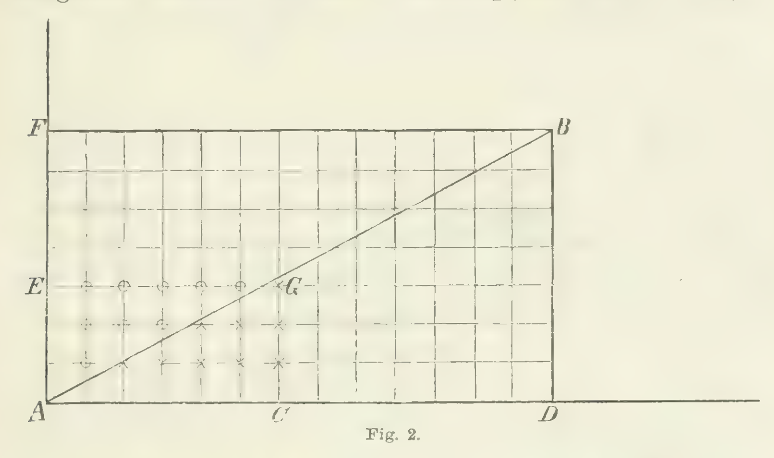


Fig. 2.

$$AC = EG = \tfrac{1}{2}(p-1), \quad AE = CG = \tfrac{1}{2}(q-1).$$

Bezeichnet jetzt μ die Anzahl der Gitterpunkte zwischen AB und der x-Axe bis zur Ordinate GC incl. (in der Figur sind diese Gitterpunkte durch Sternchen ($*$) ausgezeichnet), so ist nach dem oben Bewiesenen $\left(\frac{q}{p}\right) = (-1)^{\mu}$. Die Gleichung unserer Geraden kann aber auch

$$x = \frac{p}{q}\, y$$

geschrieben werden. Ist also ν die Anzahl der Gitterpunkte, welche zwischen AB und der y-Axe bis zur Abscisse EG incl. liegen (in der Figur sind dieselben durch kleine Nullen ($\circ$) ausgezeichnet), so ist $\left(\frac{p}{q}\right) = (-1)^{\nu}$. Man hat somit

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\mu+\nu},$$

wo $\mu + \nu$ die Anzahl aller Gitterpunkte bezeichnet, die dem

Rechteck $AEGC$ angehören. Da p prim zu q ist, so kann keiner dieser Gitterpunkte auf AB selbst liegen [nur für die Werthe $x = p, 2p, 3p, \ldots$, denen die Werthe $y = q, 2q, 3q, \ldots$ entsprechen, wird man Gitterpunkte erhalten, die auf AB liegen, der erste derselben ist also B]; die Anzahl der Gitterpunkte in $AEGC$ ist demnach

$$\mu + \nu = \tfrac{1}{2}(p-1) \cdot \tfrac{1}{2}(q-1),$$

und wir erhalten

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)},$$

was zu beweisen war.

§ 89. Zusammenstellung der gewonnenen Resultate und Anwendungen derselben. — Die in den vorhergehenden Paragraphen gewonnenen Resultate setzen uns in den Stand, in jedem Falle mit Leichtigkeit zu entscheiden, ob eine gegebene Zahl a Rest oder Nichtrest einer zweiten gegebenen Zahl m, d. h. ob die Congruenz

$$x^2 \equiv a \pmod{m}$$

möglich ist oder nicht. Zur Wiederholung und Uebung wollen wir die wichtigsten jener Ergebnisse zusammenstellen und einige Anwendungen davon machen:

I. Wenn $m = 2^\varkappa p^\lambda q^\mu \ldots$ ist, wo $p, q, \ldots$ ungerade Primzahlen, $\varkappa, \lambda, \mu, \ldots$ ganze positive Zahlen bezeichnen, so ist a nur dann Rest von m, wenn es Rest jeder der Zahlen $2^\varkappa$, p^λ, $q^\mu, \ldots$ ist (§ 80).

II. Jede ungerade Zahl a ist Rest von 2, jede Zahl a, welche die Form $4n+1$ hat, Rest von 4, endlich jede Zahl a von der Form $8n+1$ Rest von $2^\varkappa$, wenn $\varkappa > 2$ ist. Dagegen ist a Nichtrest von 4, wenn es die Form $4n+3$ hat, und Nichtrest von $2^\varkappa$ $(\varkappa > 2)$, wenn es eine der Formen

$$8n+3, \quad 8n+5, \quad 8n+7$$

hat (§ 79).

III. a ist Rest von p^λ, wenn es Rest von p ist, und Nichtrest von p^λ, wenn es Nichtrest von p ist (§ 76), also bei Anwendung des Legendre'schen Symbols

$$\left(\frac{a}{p^\lambda}\right) = \left(\frac{a}{p}\right).$$

IV. Ein Produkt ist Rest oder Nichtrest einer ungeraden Primzahl p, je nachdem es eine gerade oder eine ungerade Anzahl von Factoren, die Nichtreste sind, enthält (§ 78), also

$$\left(\frac{ab\ldots c}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{c}{p}\right).$$

V. Es ist $\left(\frac{-1}{p}\right) = +1$ oder $= -1$, je nachdem die Primzahl p die Form $4n+1$ oder $4n+3$ hat (§ 83).

VI. Es ist $\left(\frac{2}{p}\right) = +1$ für die beiden Formen $8n+1$, $8n+7$ der Primzahl p, dagegen

$\left(\frac{2}{p}\right) = -1$ für die beiden Formen $8n+3$, $8n+5$ von p (§ 84).

VII. Es ist nach § 86 $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, also $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn eine der beiden ungeraden Primzahlen die Form $4n+1$ hat, dagegen $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, wenn sowohl p, als auch q von der Form $4n+3$ ist.

I. Beispiel. Ist die Congruenz $x^2 + 80 \equiv 0 \pmod{1847}$ möglich? Ja, denn

$$\left(\frac{-80}{1847}\right) = \left(\frac{-1}{1847}\right)\left(\frac{16}{1847}\right)\left(\frac{5}{1847}\right) = (-1)(+1)(-1) = +1,$$

da $\left(\frac{-1}{1847}\right) = -1$ nach V, $16 = 4^2$ und

$$\left(\frac{5}{1847}\right) = \left(\frac{1847}{5}\right) = \left(\frac{2}{5}\right) = -1$$

nach VI ist.

II. Beispiel.

$$\left(\frac{74}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{37}{101}\right) = (-1)(+1) = -1;$$

denn $\left(\frac{2}{101}\right) = -1$, da $101 = 8 \cdot 12 + 5$ ist, und

$$\left(\frac{37}{101}\right) = \left(\frac{101}{37}\right) = \left(\frac{27}{37}\right) = \left(\frac{3^2}{37}\right)\left(\frac{3}{37}\right)$$
$$= \left(\frac{3}{37}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = +1.$$

III. Beispiel.

$$\left(\frac{-116}{839}\right) = \left(\frac{-1}{839}\right)\left(\frac{4}{839}\right)\left(\frac{29}{839}\right) = (-1)(+1)(-1) = +1;$$

denn $\left(\frac{-1}{839}\right) = -1$ nach V, $\left(\frac{4}{839}\right) = +1$, weil $4 = 2^2$ ist, und

$$\left(\frac{29}{839}\right) = \left(\frac{839}{29}\right) = \left(\frac{27}{29}\right) = \left(\frac{3^2}{29}\right)\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1 .$$

IV. Beispiel.

$$\left(\frac{73}{127}\right) = \left(\frac{127}{73}\right) = \left(\frac{54}{73}\right) = \left(\frac{9}{73}\right)\left(\frac{3}{73}\right)\left(\frac{2}{73}\right);$$

nun ist

$$\left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = +1 ,$$

und da auch

$$\left(\frac{9}{73}\right) = +1 \quad \text{und} \quad \left(\frac{2}{73}\right) = +1$$

ist, so ergiebt sich $\left(\frac{73}{127}\right) = +1$.

V. Beispiel. $\left(\frac{94}{131}\right) = \left(\frac{2}{131}\right)\left(\frac{47}{131}\right)$;

da nun $\left(\frac{2}{131}\right) = -1$ und

$$\left(\frac{47}{131}\right) = -\left(\frac{131}{47}\right) = -\left(\frac{37}{47}\right)$$
$$= -\left(\frac{47}{37}\right) = -\left(\frac{10}{37}\right) = -\left(\frac{2}{37}\right)\cdot\left(\frac{5}{37}\right),$$

und da ferner

$$\left(\frac{2}{37}\right) = -1 \quad \text{und} \quad \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1 ,$$

also

$$\left(\frac{47}{131}\right) = -(-1)(-1) = -1$$

ist, so ergiebt sich

$$\left(\frac{94}{131}\right) = (-1)(-1) = +1$$

VI. Beispiel.

$$\left(\frac{60}{227}\right) = \left(\frac{4}{227}\right)\left(\frac{3}{227}\right)\left(\frac{5}{227}\right) = -1 ;$$

denn $\left(\frac{4}{227}\right) = +1$,

$$\left(\frac{3}{227}\right) = -\left(\frac{227}{3}\right) = -\left(\frac{2}{3}\right) = +1$$

$$\left(\frac{5}{227}\right) = \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = -1 .$$

Aufgaben. 1) Zeige, dass die Congruenz $x^2 \equiv 365 \pmod{1847}$ möglich ist.

2) Ebenso, dass $x^2 \equiv 195 \pmod{1901}$ unmöglich ist.

3) Welchen Werth hat das Symbol $\left(\frac{601}{1013}\right)$? [— 1]

4) Desgl. das Symbol $\left(\frac{402}{929}\right)$? [+ 1]

§ 90. Auflösung der rein quadratischen Congruenz zweiten Grades. — Nachdem wir die Möglichkeit einer Congruenz $x^2 \equiv a \pmod{m}$ erkannt haben, liegt es uns ob, dieselbe aufzulösen. Nach § 70 dürfen wir voraussetzen, dass der Modul m nur eine einzige Primzahl in irgend einer Potenz enthalte. Der Fall, in welchem m eine Potenz von 2 ist, hat in § 79 seine Erledigung gefunden, und in § 76 ist die Aufgabe gelöst worden, die Wurzeln der Congruenz $x^2 \equiv a \pmod{p^\lambda}$ zu bestimmen, sobald die Wurzeln derselben Congruenz mod. p bekannt sind. Wir dürfen uns also auf den Fall beschränken, in welchem der Modul eine ungerade Primzahl p ist. Das Verfahren, das wir einzuschlagen haben, ist verschieden, je nachdem p die Form $4n+3$ oder $4n+1$ hat.

1. Fall. Es sei $p = 4n + 3$.

Da die Congruenz $x^2 \equiv a \pmod{p}$ möglich sein soll, so muss

$$a^{\frac{p-1}{2}}, \quad \text{d. i.} \quad a^{2n+1} \equiv +1 \pmod{p}$$

sein; hieraus folgt

$$a^{2n+1} \cdot a, \quad \text{d. i.} \quad (a^{n+1})^2 \equiv +a \pmod{p},$$

und somit sind die Wurzeln

$$x \equiv \pm a^{n+1} \pmod{p}.$$

Beispiel. Die Congruenz $x^2 \equiv 5 \pmod{11}$ ist möglich, da $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = +1$ ist. Nun ist $11 = 2 \cdot 4 + 3$, also $n = 2$, und die gesuchten Wurzeln sind

$$x \equiv \pm 5^3 \equiv \pm 125 \equiv \pm 4 \pmod{11}.$$

Wenn weiter p die Form $4n+1$ hat, so sind die Fälle $p = 8n + 1$ und $8n + 5$ zu unterscheiden.

2. Fall. Es sei $p = 8n + 5$.

Da die Congruenz möglich sein soll, so muss

$$a^{\frac{p-1}{2}}, \text{ d. i. } a^{4n+2} \equiv 1, \text{ oder } a^{4n+2} - 1 \equiv 0,$$

d. h. $$(a^{2n+1} - 1)(a^{2n+1} + 1) \equiv 0 \ (\text{mod. } p)$$

sein. Es ist also entweder

$a^{2n+1} - 1 \equiv 0$, folglich a^{2n+2}, d. i. $(a^{n+1})^2 \equiv a \ (\text{mod. } p)$, und in diesem Falle hat die Congruenz die beiden Wurzeln

$$x \equiv \pm a^{n+1} \ (\text{mod. } p);$$

oder man hat $a^{2n+1} + 1 \equiv 0$, also

$$a^{2n+2} + a \equiv 0 \ (\text{mod. } p).$$

Setzt man dann $a^{n+1} = y$, also $a^{2n+2} = y^2$, so ergiebt sich durch Addition der beiden Congruenzen $x^2 \equiv a$, $y^2 \equiv -a \ (\text{mod. } p)$

$$x^2 + y^2 \equiv 0 \ (\text{mod. } p).$$

Da die Zahl p von der Form $4n + 1$ ist, so lässt sie sich als Summe zweier Quadrate $\alpha^2 + \beta^2$ darstellen, die prim zu einander sind. Wir bezeichnen jetzt mit t, u zwei vorläufig unbestimmte Grössen; dann ist $p \ (t^2 + u^2)$, d. i.

$(\alpha^2 + \beta^2)(t^2 + u^2) = (\alpha t + \beta u)^2 + (\alpha u - \beta t)^2 \equiv 0 \ (\text{mod. } p)$, und wenn wir über t und u so verfügen, dass $\alpha u - \beta t = y$ wird, so geht diese Congruenz über in

$$(\alpha t + \beta u)^2 + y^2 \equiv 0 \ (\text{mod. } p).$$

Der Vergleich dieser Congruenz mit $x^2 + y^2 \equiv 0 \ (\text{mod. } p)$ lehrt, dass $x \equiv \pm (\alpha t + \beta u) \ (\text{mod. } p)$ ist, und dieser Ausdruck enthält die Wurzeln der vorgelegten Congruenz.

Beispiele. 1) $x^2 \equiv 20 \ (\text{mod. } 29)$.

$$\left[\left(\frac{20}{29}\right) = \left(\frac{4}{29}\right)\left(\frac{5}{29}\right) = \left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = +1\right].$$

Da $29 = 8 \cdot 3 + 5$ ist, so ist $n = 3$; wir haben also auszurechnen, ob $20^7 \equiv +1$ oder $\equiv -1 \ (\text{mod. } 29)$ ist. Es ergiebt sich der Rest $+1$, also ist $20^8 \equiv 20$, und die Congruenz hat die Wurzeln

$$x \equiv \pm 20^4 \equiv \pm 7 \ (\text{mod. } 29).$$

(2) $$x^2 \equiv 6 \ (\text{mod. } 29).$$

$\left[\left(\frac{6}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = (-1)(-1) = +1\right.$, da $\left(\frac{2}{29}\right) = -1$ und $\left.\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1 \text{ ist}\right]$.

Hier ergiebt sich $6^7 \equiv -1 \pmod{29}$, also hat, da

$$29 = 5^2 + 2^2$$

ist, die Congruenz die Wurzeln $x \equiv \pm (5t + 2u) \pmod{29}$, wofern über t und u so verfügt wird, dass

$$5u - 2t \equiv 6^4 \equiv 20 \pmod{29}$$

werde. Die Auflösung dieser Congruenz liefert der Reihe nach (§ 25)

$$2t = 5u + 29k - 20,$$

$$t = 2u + 14k - 10 + \frac{u+k}{2},$$

$$\frac{u+k}{2} = v, \quad u = 2v - k,$$

$$t = 5v + 12k - 10,$$

also

$$5t = 25v + 60k - 50,$$

$$2u = 4v - 2k,$$

$$5t + 2u = 29v + 58k - 50 \equiv -50 \equiv 8 \pmod{29},$$

und somit hat die vorgelegte Congruenz die beiden Wurzeln

$$x \equiv \pm 8 \pmod{29}.$$

3. Fall. Wenn endlich $p = 8n + 1$ ist, so lassen sich die Wurzeln der Congruenz

$$x^2 \equiv a \pmod{p},$$

die offenbar mit $x^2 \equiv a + kp \pmod{p}$ identisch ist, nur in der Weise ermitteln, dass man die Glieder der Reihe

$$a,\ a + p,\ a + 2p,\ a + 3p,\ \ldots$$

berechnet, bis man auf ein Glied stösst, welches ein vollständiges Quadrat α^2 ist. Dann sind $\pm \alpha$ die gesuchten Wurzeln.

Da $x < \frac{1}{2}p$ vorausgesetzt werden kann, also x^2, d. i. das gesuchte Quadrat $a + mp < \frac{1}{4}p^2$ ist, so ist um so mehr $mp < \frac{1}{4}p^2$, also $m < \frac{1}{4}p$, d. h. man wird nach weniger als $\frac{1}{4}p$ Versuchen zum Ziele gelangen.

Beispiele. 1) $x^2 \equiv 13 \pmod{17}$.

$$\left[\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = +1\right].$$

Es ergiebt sich die Reihe

$$13,\ 30,\ 47,\ 64,$$

also ist $$x \equiv \pm 8 \text{ (mod. 17)}.$$

(2) $$x^2 \equiv 5 \text{ (mod. 89)}.$$

$$\left[\left(\frac{5}{89}\right) = \left(\frac{89}{5}\right) = \left(\frac{1}{5}\right) = +1\right].$$

Man erhält die Reihe

$$5,\ 94,\ 183,\ 272,\ 361,$$

also ist

$$x \equiv \pm 19 \text{ (mod. 89)}.$$

Anmerkung. Auch im Falle $p = 8n + 1$ kann es vorkommen, dass die Wurzeln der Congruenz $x^2 \equiv a$ (mod. p) sich direkt bestimmen lassen. Es sei $p = 2^{\varkappa} q + 1$, wo q ungerade und $\varkappa > 3$ ist. Da a Rest von p sein soll, so ist $a^{\frac{p-1}{2}}$, d. i.

$$a^{2^{\varkappa-1} \cdot q} \equiv +1 \text{ (mod. } p).$$

In diesem Falle ist möglicherweise auch

$$a^q \equiv +1,$$

und da q ungerade ist, so können wir dann wie im Falle $p = 8n + 5$ verfahren.

Beispiele. 1) $x^2 \equiv 10$ (mod. 41).

$$\left[\left(\frac{10}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{5}{41}\right) = (+1)\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = +1\right].$$

Es ist also 10^{20}, d. i. $10^{4 \cdot 5} \equiv +1$ (mod. 41).

Nun ergiebt aber die Rechnung, dass $10^5 \equiv +1$, also $10^6 \equiv +10$ (mod. 41) ist; somit hat die Congruenz die beiden Wurzeln

$$x \equiv \pm 10^3 \equiv \pm 16 \text{ (mod. 41)}.$$

2) $x^2 \equiv 41$ (mod. 73).

$$\left[\left(\frac{41}{73}\right) = \left(\frac{73}{41}\right) = \left(\frac{32}{41}\right) = \left(\frac{16}{41}\right)\left(\frac{2}{41}\right) = +1\right].$$

Es ist also jedenfalls $41^{36} \equiv +1$ (mod. 73).

Nun ergiebt sich, dass schon $41^9 \equiv -1$, also

$$41^{10} \equiv -41 \text{ (mod. 73)}$$

ist. Wir setzen daher $41^5 = y$ und kommen dadurch zu der Congruenz $x^2 + y^2 \equiv 0$ (mod. 73), welche, da $73 = 8^2 + 3^2$ ist, die Wurzeln

$$x \equiv \pm (8t + 3u) \text{ (mod. 73)}$$

hat, wofern über t, u so verfügt wird, dass $8u - 3t \equiv y$, d. h. $\equiv 41^5$ (mod. 73) werde. 41^5 ist $\equiv 18$, und durch Auflösung der Congruenz $8u - 3t \equiv 18$ (mod. 73) ergeben sich die Werthe

$$x \equiv \pm 25 \pmod{73};$$

dies sind die Wurzeln der vorgelegten Congruenz.

§ 91. Auflösung der Congruenz $x^2 \equiv a$ (mod. p) durch die Methode der Ausschliessung (Gauss, Disquisitiones, 319 ff.). — Das im vorigen Paragraphen für den Fall $p = 8n + 1$ angewandte Verfahren, welches natürlich auch für jede andere Form von p eingehalten werden kann, ist einer seine Brauchbarkeit bedeutend erhöhenden Abkürzung fähig, die darin besteht, dass man nicht alle Glieder der Reihe

$$a,\ a + p,\ a + 2p,\ \ldots$$

bis zu einem Gliede berechnet, welches eine Quadratzahl ist, sondern zunächst von den Gliedern, die unmöglich eine Lösung liefern können, möglichst viele ausscheidet.

Wir haben schon gesehen, dass wir die Wurzel x der vorgelegten Congruenz, d. i. die Wurzel der unbestimmten Gleichung

$$x^2 = a + kp,$$

in welcher k eine ganze Zahl bezeichnet, als $< \frac{1}{2}p$ voraussetzen können. Dann ist x^2, d. i. $a + kp < \frac{1}{4}p^2$, also

$$k < \frac{p}{4} - \frac{a}{p}.$$

Da ausserdem $a + kp = x^2$, also positiv sein muss, so muss $k > -\frac{a}{p}$ sein, und somit liegt k zwischen $-\frac{a}{p}$ und $\frac{p}{4} - \frac{a}{p}$.

Es sei nun E eine beliebige zwischen diesen Grenzen liegende ganze Zahl, die prim zu p und > 2 ist, und diese Zahl habe die Nichtreste n_1, n_2, ..., welche sämmtlich als verschieden, d. h. in Beziehung auf den Modul E incongruent vorausgesetzt werden. Wir bilden dann die Congruenzen

$$a + kp \equiv n_1,\ a + kp \equiv n_2,\ \ldots \pmod{E},$$

welche beziehungsweise die Wurzeln k_1, k_2, ... haben mögen, die wir als positiv und $< E$ voraussetzen. Wenn wir nun für k irgend einen Werth setzen, welcher einer der Zahlen k_1, k_2, ... in Beziehung auf den Modul E congruent ist, so wird

der für $a + kp$ sich ergebende Werth einer der Zahlen n_1, n_2, ... congruent, also ein Nichtrest von E, folglich jedenfalls keine Quadratzahl sein. Wir können somit von den Zahlen, welche zwischen den für k ermittelten Grenzen liegen, alle diejenigen als unnütz ausschliessen, welche von den Formen $k_1 + Et$, $k_2 + Et$, ... sind.

Wählen wir weiter eine beliebige andere Zahl $E' > 2$, welche die verschiedenen (mod. E' incongruenten) Nichtreste n_1', n_2', ... haben möge, so gelangen wir durch nochmalige Anwendung des dargelegten Verfahrens zur Ausschliessung aller Zahlen der Formen

$$k_1' + E't,\ k_2' + E't,\ \ldots,$$

wo k_1', k_2', ... beziehungsweise die Wurzeln der Congruenzen

$$a + pk' \equiv n_1',\ a + pk' \equiv n_2',\ \ldots \pmod{E'}$$

sind und t eine unbestimmte ganze Zahl bezeichnet.

So können wir fortfahren, bis die Anzahl der stehen gebliebenen Zahlen so klein geworden ist, dass es bequemer scheint, jede derselben in dem Ausdruck $a + kp$ an die Stelle von k zu setzen und zu sehen, ob dadurch eine Quadratzahl entsteht, als das dargelegte Ausschliessungsverfahren nochmals anzuwenden.

1. Beispiel. Die Congruenz $x^2 \equiv 22 \pmod{97}$ ist der unbestimmten Gleichung

$$x^2 = 22 + 97k$$

äquivalent, und es ergeben sich für k die Grenzen $-\frac{22}{97}$ und $\frac{97}{4} - \frac{22}{97}$. Da der Werth $k = 0$ nicht in Betracht kommt, weil 22 keine Quadratzahl ist, so enthält das Gebiet, das wir zu betrachten haben, die Zahlen 1, 2, 3, ..., 24.

Wir nehmen nun erstens $E = 3$ an. Diese Zahl hat nur den einen Nichtrest 2, und da die Congruenz

$$22 + 97k \equiv 2 \pmod{3}$$

die Wurzel $k \equiv 1 \pmod{3}$ hat, so sind alle Zahlen von der Form $1 + 3t$, d. i.

1, 4, 7, 10, 13, 16, 19, 22

auszuschliessen.

Zweitens nehmen wir $E = 4$; diese Zahl hat die Nichtreste 2, 3, und die Congruenzen

$$22 + 97k \equiv 2, \; 22 + 97k \equiv 3 \pmod{4}$$

haben beziehungsweise die Wurzeln

$$k \equiv 0, \; k \equiv 1 \pmod{4};$$

daher sind weiter alle Zahlen der Formen

$$4t, \; 4t + 1, \text{ also } 8, 12, 20, 24 \text{ und } 5, 9, 17, 21$$

auszuschliessen.

Drittens nehmen wir $E = 5$ an; diese Zahl hat die Nichtreste 2, 3, und da die Congruenzen

$$22 + 97k \equiv 2, \; 22 + 97k \equiv 3 \pmod{5}$$

beziehungsweise die Wurzeln

$$k \equiv 0, \; k \equiv 3 \pmod{5}$$

haben, so fallen auch die Zahlen der Formen $5t$ und $3 + 5t$, d. i. 15 und 3, 18, 23 weg.

Wenn wir jetzt $E = 6$ annehmen wollten, so würden wir zur Ausschliessung von Zahlen gelangen, die schon für $E = 3$ in Wegfall gekommen sind; den Grund dafür werden wir weiter unten kennen lernen. Wir setzen daher viertens $E = 7$. Diese Zahl hat die Nichtreste 3, 5, 6, und die Congruenzen

$$22 + 97k \equiv 3, \; 22 + 97k \equiv 5, \; 22 + 97k \equiv 6 \pmod{7}$$

haben beziehungsweise die Wurzeln

$$k \equiv 5, \; k \equiv 3, \; k \equiv 2 \pmod{7}.$$

Es sind also die Zahlen der Formen $5 + 7t$, $3 + 7t$, $2 + 7t$, d. i. 2 auszuschliessen (die übrigen Zahlen dieser Formen sind schon weggefallen). Da von den 24 Zahlen, um die es sich handelte, jetzt nur noch die drei Zahlen 6, 11, 14 stehen geblieben sind, so verlohnt es sich nicht, das Ausschliessungsverfahren nochmals vorzunehmen. Die Einsetzung dieser drei Werthe in $22 + 97k$ an die Stelle von k liefert beziehungsweise 604, 1089, 1380. Die zweite dieser drei Zahlen ist eine Quadratzahl, nämlich 33^2; unsere Congruenz $x^2 \equiv 22 \pmod{97}$ hat also die beiden Wurzeln $x \equiv \pm 33 \pmod{97}$.

2. **Beispiel.** $x^2 \equiv 264 \pmod{367}$.

[$264 = 4 \cdot 66$, $367 = 8 \cdot 45 + 7$,

also

$$\left(\frac{264}{367}\right) = \left(\frac{66}{367}\right) = \left(\frac{2}{367}\right)\left(\frac{3}{367}\right)\left(\frac{11}{367}\right) = \left(\frac{3}{367}\right)\left(\frac{11}{367}\right) = +1,$$

da
$$\left(\frac{3}{367}\right) = -\left(\frac{367}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

und
$$\left(\frac{11}{367}\right) = -\left(\frac{367}{11}\right) = -\left(\frac{4}{11}\right) = -1 \text{ ist}].$$

Wir beschäftigen uns mit der Gleichung

$$x^2 = 264 + 367k$$

und erhalten für k zunächst die Grenzen

$$-\frac{264}{367} \quad \text{und} \quad \frac{367}{4} - \frac{264}{367};$$

also muss, da der Werth 0 wieder ausgeschlossen bleibt, k eine der Zahlen 1, 2, 3, ..., 91 sein.

Nun werden durch die Wurzel $k \equiv 2 \pmod{3}$ der Congruenz $264 + 367k \equiv 2 \pmod{3}$ zunächst die 30 Zahlen der Form $2 + 3t$, also

2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35,
38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77,
80, 83, 86, 89

ausgeschlossen, so dass noch 61 Zahlen zurückbleiben.

Weiter haben die beiden Congruenzen $264 + 367k \equiv 2$ oder $\equiv 3 \pmod{4}$ beziehungsweise die Wurzeln $k \equiv 1$ und $k \equiv 2 \pmod{4}$, und daher fallen auch die Zahlen $1 + 4t$ und $2 + 4t$ weg; von den noch gebliebenen sind dies die 30 Zahlen

1, 6, 9, 10, 13, 18, 21, 22, 25, 30,
33, 34, 37, 42, 45, 46, 49, 54, 57, 58,
61, 66, 69, 70, 73, 78, 81, 82, 85, 90,

so dass noch 31 Zahlen zurückbleiben.

Drittens lösen wir die beiden Congruenzen

$$264 + 367k \equiv 2 \quad \text{oder} \quad \equiv 3 \pmod{5}$$

und erhalten beziehungsweise die Wurzeln

$$k \equiv 4 \quad \text{und} \quad k \equiv 2 \pmod{5}.$$

Daher sind auch die Zahlen der Formen $2 + 5t$, $4 + 5t$ auszuschliessen. Es sind dies die 14 Zahlen

$$4, 7, 12, 19, 24, 27, 39, 52, 64, 67,$$
$$72, 79, 84, 87,$$

so dass noch 17 Zahlen zurückbleiben.

Viertens fallen, da die drei Congruenzen

$$264 + 367k \equiv 3 \quad \text{oder} \quad \equiv 5 \quad \text{oder} \quad \equiv 6 \pmod{7}$$

beziehungsweise die Wurzeln

$$k \equiv 4, \ k \equiv 0, \ k \equiv 5 \pmod{7}$$

haben, auch die Zahlen der Formen $7t$, $4 + 7t$, $5 + 7t$ weg; es sind dies die 7 Zahlen 28, 40, 60, 63, 75, 88, 91, so dass noch 10 Zahlen zurückbleiben.

So fortfahrend scheiden wir durch Benutzung der Nichtreste 3, 5, 7 von 8 noch die Zahlen 3, 43, 51, durch Benutzung der Nichtreste von 9 noch 36 und 48, endlich durch Benutzung der Nichtreste von 11 noch die Zahl 76 aus. Es bleiben dann noch die 4 Zahlen 15, 16, 31, 55. Für diese Werthe von k wird der Ausdruck $264 + 367k$ beziehungsweise gleich

$$5769, 6136, 11641, 20449.$$

Die letzte dieser Zahlen ist $= 143^2$, und somit hat unsere Congruenz die Wurzeln

$$x \equiv \pm 143 \pmod{367}.$$

Anmerkungen. 1. Die Zahlen $E, E', \ldots$, die wir der Reihe nach zur Ausschliessung der Zahlen benutzen, welche, in den Ausdruck $a + kp$ an die Stelle von k gesetzt, kein Quadrat liefern, nennen wir nach Gauss die ausschliessenden Zahlen. Nun erfolgt diese Ausschliessung durch Lösung von Congruenzen $a + kp \equiv n \pmod{E}$, wo n einen Nichtrest von E bezeichnet; jeder einem auszuscheidenden k entsprechende Werth von $a + kp$ ist daher gleichfalls ein Nichtrest von E, während die durch diesen Ausdruck darstellbaren Reste von E nicht berührt werden. Wenn daher E eine ungerade Zahl ist, in welchem Falle E und $2E$ dieselben Reste und dieselben Nichtreste haben (die Zahl 2 besitzt keine Nichtreste), so wird die Anwendung von $2E$ als ausschliessende Zahl keinen anderen Erfolg als die von E haben. Hat man also 3, 5, 7, ... als ausschliessende Zahlen bereits benutzt, so können 6, 10, 14, ... übergangen werden.

2. Weiter ist ersichtlich, dass, wenn man nach einander E, E' als ausschliessende Zahlen anwendet, alle diejenigen Werthe des Ausdrucks $a + kp$ entfernt werden, welche Nichtreste einer der beiden Zahlen E, E' oder beider zugleich sind, so dass nur diejenigen bleiben, welche Reste jeder dieser beiden Zahlen sind. Da nun, wenn E, E' keinen gemeinschaftlichen Factor haben, jene ausgeschiedenen Zahlen sämmtlich Nichtreste und die gebliebenen sämmtlich Reste des Produkts EE' sind, so würde die Anwendung dieses Produkts als ausschliessende Zahl nur solche Zahlen entfernen, die schon durch Anwendung von E und E' beseitigt sind; es würde also die Anwendung von EE' ganz überflüssig sein, und wir sehen somit, dass es genügt, nur Primzahlen und Potenzen von Primzahlen zu ausschliessenden Zahlen zu nehmen.

§ 92. Die Congruenz $x^2 \equiv a \pmod{m}$, wenn a nicht prim zu m ist. — Wir haben bisher immer vorausgesetzt, dass a und m relative Primzahlen seien. Haben nun a und m einen von 1 verschiedenen grössten gemeinschaftlichen Divisor d, ist etwa $a = \alpha d$, $m = \mu d$, so muss, da $x^2 - a$ durch m theilbar sein soll, $x^2 - a$ sicherlich auch durch d theilbar sein, also, da a den Factor d enthält, x^2 durch d theilbar sein. Wenn daher $d = d_1^2 d_2$ ist, wo d_2 durch keine Quadratzahl theilbar sein soll, so wird x durch $d_1 d_2$ theilbar sein müssen, und die vorgelegte Congruenz geht in Folge der Substitution

$$x = d_1 d_2 y$$

über in

$$d_1^2 d_2^2 y^2 \equiv \alpha d_1^2 d_2 \pmod{\mu d_1^2 d_2}.$$

Hieraus folgt durch Division mit $d_1^2 d_2$

$$d_2 y^2 \equiv \alpha \pmod{\mu},$$

und da α prim zu μ ist, so ist die vorgelegte Congruenz auf eine andere von der Art der bisher betrachteten zurückgeführt. Hat man mittels der letzten Congruenz y bestimmt, so liefert die Relation $x = d_1 d_2 y$ die Werthe von x.

Beispiele. I. $\quad x^2 \equiv 3 \pmod{6}$.

Wir setzen $x = 3y$ und erhalten sofort

$$3y^2 \equiv 1 \pmod{2},$$

$$y \equiv +1 \pmod{2},$$

$$x \equiv +3 \pmod{6}.$$

II. $$x^2 \equiv 16 \pmod{28}.$$

Wir setzen $x = 2y$ und erhalten
$$y^2 \equiv 4 \pmod{7}.$$
Es ist also
$$y \equiv \pm 2 \pmod{7}$$
und
$$x \equiv \pm 4 \pmod{14},$$
so dass sich als Wurzeln der Congruenz ± 4 und ± 18 ergeben.

III. $$x^2 \equiv 900 \pmod{2475}.$$

Da $900 = 2^2 \cdot 3^2 \cdot 5^2$ und $2475 = 3^2 \cdot 5^2 \cdot 11$ ist, so ist $d = 3^2 \cdot 5^2$; wir setzen also
$$x = 15y$$
und erhalten
$$225y^2 \equiv \quad 900 \pmod{2475}$$
oder
$$y^2 \equiv + \quad 4 \pmod{11},$$
$$y \equiv \pm \quad 2 \pmod{11},$$
$$x \equiv \pm \quad 30 \pmod{165}.$$

Es ergeben sich also die 30 für den Modul 2475 incongruenten Wurzeln

$$\pm 30, \pm 195, \pm 360, \pm 525, \pm 690, \pm 855,$$
$$\pm 1020, \pm 1185, \pm 1350, \pm 1515, \pm 1680,$$
$$\pm 1845, \pm 2010, \pm 2175, \pm 2340.$$

IV. $$x^2 \equiv 76 \pmod{684}.$$

Da $76 = 2^2 \cdot 19$, $684 = 2^2 \cdot 3^2 \cdot 19$ ist, so ist $d = 2^2 \cdot 19$. Wir setzen also
$$x = 2 \cdot 19y$$
und erhalten
$$2^2 \cdot 19^2 y^2 \equiv 2^2 \cdot 19 \pmod{2^2 \cdot 3^2 \cdot 19},$$
$$19y^2 \equiv \quad 1 \pmod{9},$$
$$y^2 \equiv \quad 1 \pmod{9},$$
$$y \equiv \pm \ 1 \pmod{9},$$
$$x \equiv \pm 38 \pmod{342},$$

und die 4 Wurzeln der vorgelegten Congruenz sind
$$\pm 38, \pm 380.$$

§ 93. Formen für die Primzahlen, von denen eine gegebene Zahl Rest oder Nichtrest ist. — Der Reciprocitätssatz setzt uns in den Stand, allgemein die Frage zu beantworten, für welche Primzahlen p die Congruenz $x^2 \equiv a$, in der a eine gegebene Zahl bezeichnet, möglich, und für welche sie unmöglich ist.

I. Es sei zunächst a gleichfalls eine Primzahl und zwar von der Form $4n+1$. Wenn unsere Congruenz bestehen soll, so muss $\left(\frac{a}{p}\right)$, d. i. aber nach dem Reciprocitätssatz $\left(\frac{p}{a}\right)$, den Werth $+1$ haben, also p Rest von a sein. Werden nun die Reste von a mit $r_1, r_2, \ldots, r_\varkappa$, die Nichtreste mit $n_1, n_2, \ldots, n_\varkappa$ bezeichnet, und stellt k eine unbestimmte ganze Zahl dar, so ist die Congruenz $x^2 \equiv a$ möglich für alle in den Formen

$$(1) \qquad ak + r_1,\; ak + r_2,\; \ldots,\; ak + r_\varkappa$$

enthaltenen Primzahlen p, unmöglich für alle Primzahlen der Formen

$$(2) \qquad ak + n_1,\; ak + n_2,\; \ldots,\; ak + n_\varkappa.$$

Wenn aber $x^2 \equiv a \pmod{p}$ ist, so geht p ohne Rest in $x^2 - a$ auf; daher nennt man die Glieder der arithmetischen Reihen (1) die Formen der Divisoren von $x^2 - a$ und dementsprechend die Glieder von (2) die Formen der Nichtdivisoren von $x^2 - a$.

Beispiel. Da 13 die Reste 1, 3, 4, 9, 10, 12, die Nichtreste 2, 5, 6, 7, 8, 11 hat, so sind

$$13k + 1,\quad 13k + 3,\quad 13k + 4,\quad \ldots,\quad 13k + 12$$

die Formen der Divisoren, dagegen

$$13k + 2,\quad 13k + 5,\quad \ldots,\quad 13k + 11$$

die Formen der Nichtdivisoren von $x^2 - 13$, d. h. für jede Primzahl einer Form der ersten Gruppe als Modul ist die Congruenz $x^2 \equiv 13$ möglich, für jede Primzahl der zweiten Gruppe ist sie es nicht. Von der ersteren Art sind z. B. die Primzahlen 3, 17, 23, 29, 43, 53, 61, 79, ..., und die Indextafeln lehren in der That, dass für jede dieser Zahlen als Modul der Index von 13 gerade ist. Von der zweiten Art sind 5, 7, 11,

19, 31, 37, 41, 47, 59, 67, 71, 73, 83, 89, 97, ..., und für jede dieser Zahlen als Modul ist der Index von 13 ungerade.

II. Ganz ebenso gestaltet sich die Sache, wenn a von der Form $4n + 3$, aber negativ ist, wenn also die Congruenz $x^2 \equiv -a$ vorliegt. Es muss dann $\left(\frac{-a}{p}\right)$, d. i.

$$\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = +1$$

sein; wenn also erstens p die Form $4n + 1$ beigelegt wird, wodurch $\left(\frac{-1}{p}\right) = +1$ wird, so muss $\left(\frac{a}{p}\right)$, d. i. aber in Folge unserer Annahme $\left(\frac{p}{a}\right) = +1$ sein; und wenn zweitens p die Form $4n + 3$ beigelegt wird, wodurch $\left(\frac{-1}{p}\right) = -1$ wird, so muss $\left(\frac{a}{p}\right)$, d. i. bei der jetzigen Voraussetzung

$$-\left(\frac{p}{a}\right) = -1,$$

also $\left(\frac{p}{a}\right)$ gleichfalls $= +1$ sein. Werden also wieder die Reste von $+a$ mit $r_1, r_2, \ldots, r_\varkappa$, die Nichtreste mit $n_1, n_2, \ldots, n_\varkappa$ bezeichnet, so sind

$$ak + r_1, \quad ak + r_2, \quad \ldots, \quad ak + r_\varkappa$$

die Formen der Divisoren und

$$ak + n_1, \quad ak + n_2, \quad \ldots, \quad ak + n_\varkappa$$

die Formen der Nichtdivisoren von $x^2 + a$.

Beispiel. $x^2 + 19$ hat zu Divisoren alle Primzahlen der 9 Formen

$$19k + 1, 4, 5, 6, 7, 9, 11, 16, 17,$$

zu Nichtdivisoren alle Primzahlen der Formen

$$19k + 2, 3, 8, 10, 12, 13, 14, 15, 18.$$

Man überzeuge sich, dass Ind. (-19) für die Primzahlen der ersten Art als Moduln gerade, für die der zweiten Art ungerade ist.

III. Es sei jetzt a eine Primzahl von der Form $4n + 1$, aber negativ genommen, also die Congruenz $x^2 \equiv -a$ vorgelegt. Da

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = +1$$

sein soll, und $\left(\frac{-1}{p}\right) = +1$ oder $= -1$ ist, je nachdem p die Form $4n+1$ oder $4n+3$ hat, so muss $\left(\frac{a}{p}\right)$, d. i. hier $\left(\frac{p}{a}\right)$ im ersteren Falle $= +1$, im zweiten $= -1$ sein, oder, unter Beibehaltung der früheren Bezeichnung, x^2+a hat zu Divisoren alle Primzahlen der Form $4n+1$, welche den Formen

$$ak+r_1,\quad ak+r_2,\quad \ldots,\quad ak+r_\varkappa,$$

sowie alle Primzahlen der Form $4n+3$, welche den Formen

$$ak+n_1,\quad ak+n_2,\quad \ldots,\quad ak+n_\varkappa$$

angehören; dagegen hat x^2+a die Primzahlen $4n+3$ der Formen $ak+r_1, \ldots, ak+r_\varkappa$, sowie die Primzahlen $4n+1$ der Formen $ak+n_1, \ldots, ak+n_\varkappa$ zu Nichtdivisoren.

IV. Wenn endlich a eine positiv genommene Primzahl von der Form $4n+3$ ist, so ist

$$\left(\frac{a}{p}\right) = +\left(\frac{p}{a}\right) \quad \text{oder} \quad = -\left(\frac{p}{a}\right),$$

je nachdem p als von der Form $4n+1$ oder $4n+3$ vorausgesetzt wird. Nun soll $\left(\frac{a}{p}\right) = +1$ sein, also ist im ersteren Falle auch $\left(\frac{p}{a}\right) = +1$, im zweiten $-\left(\frac{p}{a}\right) = +1$, folglich $\left(\frac{p}{a}\right) = -1$, so dass wir zu genau demselben Ergebniss wie in III gelangen.

Beispiel. x^2-19 hat zu Divisoren alle Primzahlen $4n+1$ der 9 Formen $19k+1$, 4, 5, 6, 7, 9, 11, 16, 17, sowie alle Primzahlen $4n+3$ der 9 Formen

$$19k+2,\ 3,\ 8,\ 10,\ 12,\ 13,\ 14,\ 15,\ 18,$$

dagegen zu Nichtdivisoren alle Primzahlen $4n+3$ der ersteren Gruppe von Formen, sowie alle Primzahlen $4n+1$ der zweiten Gruppe.

Anmerkung. Die Zahlen p sind in den Fällen III und IV zwei Bedingungen unterworfen (dass sie mod. 4 einen Rest 1 oder 3 und mod. a einen Rest r_1 oder $r_2, \ldots,$ oder $n_1, \ldots$ geben sollen); diese beiden Bedingungen lassen sich, wie wir § 24, III gesehen haben, in eine einzige vereinigen. Wenden wir das dort dargelegte Verfahren auf das letzte Bei-

spiel an, so ergeben sich als Formen der Divisoren von $x^2 - 19$ (nach der Grösse der Reste geordnet)

$$76k + 1, 3, 5, 9, 15, 17, 25, 27, 31, 45,$$
$$49, 51, 59, 61, 67, 71, 73, 75,$$

als Formen der Nichtdivisoren

$$76k + 7, 11, 13, 21, 23, 29, 33, 35, 37, 39,$$
$$41, 43, 47, 53, 55, 63, 65, 69.$$

[Man bestätige dies durch Betrachtung der Indices].

§ 94. Fortsetzung. Die gegebene Zahl a ist zusammengesetzt. — Aehnliche Formeln giebt es für die Divisoren und Nichtdivisoren von $x^2 - a$, wenn a eine beliebig zusammengesetzte Zahl ist. Man sieht aber leicht, dass man nur solche Zahlen a zu betrachten hat, welche durch kein Quadrat theilbar sind. Ist nämlich $a = \mathfrak{a}^2 a'$, so werden, da $\left(\frac{\mathfrak{a}^2 a'}{p}\right) = \left(\frac{a'}{p}\right)$ ist, alle Divisoren von $x^2 - a$ auch Divisoren von $x^2 - a'$ sein und alle Nichtdivisoren von $x^2 - a$ auch Nichtdivisoren von $x^2 - a'$. Wir dürfen also voraussetzen, a enthalte jeden seiner Primfactoren nur in der ersten Potenz, und unterscheiden dann folgende drei Fälle:

I. a ist von der Form $+(4n + 1)$ oder $-(4n + 3)$;

II. a hat eine der beiden Formen

$$-(4n + 1), \quad +(4n + 3);$$

III. a hat eine der beiden Formen $\pm 2n$, wo n eine ungerade Zahl ist.

I. Fall. Wir zerlegen a in seine Primfactoren, die mit $\alpha, \beta, \gamma, \ldots$ bezeichnet werden mögen, und setzen vor jeden Primfactor, der die Form $4n + 3$ hat, das Zeichen $-$. Da eine gerade Anzahl Factoren der Form $4n + 3$ ein Produkt von der Form $4n + 1$, eine ungerade Anzahl dagegen ein Produkt von der Form $4n + 3$ liefert, so bilden die Zahlen $\alpha, \beta, \gamma, \ldots$, auch nachdem einige das Zeichen $-$ erhalten haben, noch das Produkt a.

Nun vertheilen wir die $\varphi(a)$ Zahlen, die prim zu a und kleiner als a sind, in 2 Klassen. In die erste Klasse stellen wir alle Zahlen, welche Nichtreste einer geraden Anzahl der Factoren $\alpha, \beta, \gamma, \ldots$, oder Nichtreste keines derselben sind,

in die zweite Klasse alle diejenigen, welche Nichtreste einer ungeraden Anzahl der Factoren $\alpha, \beta, \gamma, \ldots$ sind. Werden die Zahlen der ersten Klasse mit $r_1, r_2, \ldots$, die der zweiten mit $n_1, n_2, \ldots$ bezeichnet, so sind

$$ak + r_1, \quad ak + r_2, \ldots$$

die Formen der Divisoren,

$$ak + n_1, \quad ak + n_2, \ldots$$

die Formen der Nichtdivisoren von $x^2 - a$; denn, wenn die Congruenz $x^2 \equiv a \pmod{p}$ bestehen soll, so muss

$$\left(\frac{a}{p}\right), \text{ d. i. } \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right)\left(\frac{\gamma}{p}\right)\cdots = +1$$

sein, folglich muss die Anzahl der Factoren dieses Produkts, die den Werth -1 haben, eine gerade sein.

1. **Beispiel.** Um die Formen der Divisoren von $x^2 - 21$ zu finden, setzen wir $21 = (-3)(-7)$. Nun hat unter den $\varphi(21) = 12$ Zahlen, die prim zu 21 und < 21 sind,

3 die Nichtreste 2, 5, 8, 11, 17, 20,

7 die Nichtreste 5, 10, 13, 17, 19, 20.

Nichtreste beider Zahlen 3, 7 oder keiner derselben sind also 1, 4, 5, 16, 17, 20;

dagegen sind Nichtreste nur einer dieser Zahlen 2, 8, 10, 11, 13, 19.

Die Congruenz $x^2 \equiv 21 \pmod{p}$ ist also möglich für jede Primzahl p einer der Formen

$$21k + 1,\ 4,\ 5,\ 16,\ 17,\ 20,$$

unmöglich für jede Primzahl einer der Formen

$$21k + 2,\ 8,\ 10,\ 11,\ 13,\ 19.$$

Es empfiehlt sich, die Bedingung, dass p ungerade sein soll, auch in dem Resultat zum Ausdruck zu bringen. Das geschieht, indem wir die gefundenen Formen noch der Bedingung $p = 2n + 1$ unterwerfen (vgl. die Anmerkung zum vorhergehenden Paragraphen). Wir erhalten dann leicht als Formen der Divisoren von $x^2 - 21$

$$42k + 1,\ 5,\ 17,\ 25,\ 37,\ 41$$

und als Formen der Nichtdivisoren

$$42k + 11,\ 13,\ 19,\ 23,\ 29,\ 31.$$

2. Beispiel. $x^2 \equiv -15 \pmod{p}$.

$$(-15) = (-3)(+5).$$

Unter den $\varphi(15) = 8$ Zahlen, die prim zu 15 und < 15 sind, hat

3 die Nichtreste 2, 8, 11, 14,

5 die Nichtreste 2, 7, 8, 13.

Es sind also Nichtreste beider Zahlen 3, 5 oder keiner derselben 1, 2, 4, 8,

Nichtreste nur einer derselben 7, 11, 13, 14.

Daher sind $15k + 1, 2, 4, 8$ die Formen der Divisoren, $15k + 7, 11, 13, 14$ die Formen der Nichtdivisoren von $x^2 + 15$.

Bringen wir auch hier die Bedingung $p = 2n + 1$ zum Ausdruck, so erhalten wir leicht als Formen der Divisoren von $x^2 + 15$

$$30k + 1,\ 17,\ 19,\ 23$$

und als Formen der Nichtdivisoren

$$30k + 7,\ 11,\ 13,\ 29.$$

II. Fall. Wenn a eine der beiden Formen

$$-(4n+1), \quad +(4n+3)$$

hat, so können wir $a = (-1)\,a'$ setzen, wo a' eine Zahl einer der im ersten Falle behandelten Formen ist. Da dann

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a'}{p}\right)$$

ist, so wird $\left(\frac{a}{p}\right) = +1$ sein, erstens, wenn $\left(\frac{-1}{p}\right) = +1$ und zugleich $\left(\frac{a'}{p}\right) = +1$ ist, zweitens, wenn jedes der Symbole $\left(\frac{-1}{p}\right)$, $\left(\frac{a'}{p}\right)$ den Werth -1 hat; dagegen wird $\left(\frac{a}{p}\right) = -1$ sein, wenn das eine dieser Symbole $= +1$, das andere $= -1$ ist.

Haben wir also nach dem Vorhergehenden die Formen der Divisoren und die der Nichtdivisoren von $x^2 - a'$ bestimmt, und werden die ersteren mit

(1) $$ak + r_1, \quad ak + r_2, \ldots,$$

die letzteren mit

(2) $$ak + n_1, \quad ak + n_2, \ldots$$

bezeichnet, so sind alle in den Formen (1) enthaltenen Primzahlen der Form $4n + 1$ und alle in den Formen (2) enthaltenen Primzahlen der Form $4n + 3$ Divisoren, dagegen alle in den Formen (1) enthaltenen Primzahlen der Form $4n + 3$, sowie alle in den Formen (2) enthaltenen Primzahlen $4n + 1$ Nichtdivisoren von $x^2 - a$.

Die beiden Bedingungen, denen die Divisoren, wie auch die Nichtdivisoren unterworfen sind, lassen sich in der oben angegebenen Weise leicht in einen Ausdruck vereinigen, wodurch man eine Reihe Formen für alle Divisoren, eine zweite Reihe Formen für alle Nichtdivisoren erhält.

Beispiel. Es sollen die Formen der Divisoren und die der Nichtdivisoren von $x^2 - 15$ bestimmt werden. Wie wir oben gefunden haben, sind die Formen der Divisoren von $x^2 + 15$

(1) $$30k + 1,\ 17,\ 19,\ 23$$

und die Formen der Nichtdivisoren von $x^2 + 15$

(2) $$30k + 7,\ 11,\ 13,\ 29\,.$$

Folglich hat $x^2 - 15$ zu Divisoren alle in (1) enthaltenen Primzahlen der Form $4n + 1$ und alle in (2) enthaltenen Primzahlen der Form $4n + 3$, d. i. alle Primzahlen der Formen

$$60k + 1,\ 7,\ 11,\ 17,\ 43,\ 49,\ 53,\ 59,$$

und zu Nichtdivisoren alle in (1) enthaltenen Primzahlen der Form $4n + 3$ und alle in (2) enthaltenen Primzahlen der Form $4n + 1$, d. i. alle Primzahlen der Formen

$$60k + 13,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 47\,.$$

III. Im dritten Falle endlich dürfen wir $a = (\pm 2)\,a'$ voraussetzen, wo a' eine ungerade Zahl einer der im Falle I betrachteten Formen ist.

Es ist dann $\left(\frac{a}{p}\right)$, d. i. $\left(\frac{\pm 2}{p}\right)\left(\frac{a'}{p}\right) = +\,1$, wenn jedes der Symbole $\left(\frac{\pm 2}{p}\right)$, $\left(\frac{a'}{p}\right)$ den Werth $+\,1$ oder den Werth $-\,1$ hat, dagegen $\left(\frac{a}{p}\right) = -\,1$, wenn das eine der Symbole

$\left(\frac{\pm 2}{p}\right)$, $\left(\frac{a'}{p}\right)$ gleich $+1$, das andere gleich -1 ist. Nun ist nach § 84

$$\left(\frac{+2}{p}\right) = +1 \text{ für die Primzahlen der Formen } 8n+1,\ 8n+7,$$
$$= -1 \quad \text{,, ,, ,, ,, ,,} \quad 8n+3,\ 8n+5,$$

und

$$\left(\frac{-2}{p}\right) = +1 \quad \text{,, ,, ,, ,, ,,} \quad 8n+1,\ 8n+3,$$
$$= -1 \quad \text{,, ,, ,, ,, ,,} \quad 8n+5,\ 8n+7.$$

Sind also die Formen der Divisoren von $x^2 - a'$

$$(1) \qquad ak + r_1,\quad ak + r_2,\ \ldots$$

und die der Nichtdivisoren dieses Ausdrucks

$$(2) \qquad ak + n_1,\quad ak + n_2,\ \ldots$$

nach dem Früheren bestimmt, so sind die Divisoren von $x^2 - a$, wenn $a = (+2)\,a'$ ist, alle Primzahlen der Formen $8n+1$, $8n+7$, welche sich in den Formen (1) vorfinden, und alle Primzahlen der Formen $8n+3$, $8n+5$, welche in den Formen (2) enthalten sind; Nichtdivisoren sind in diesem Falle alle Primzahlen der Formen $8n+3$, $8n+5$, welche die Formen (1) enthalten, und alle Primzahlen $8n+1$, $8n+7$, welche die Formen (2) enthalten.

Ist dagegen $a = (-2)\,a'$, so sind alle Primzahlen $8n+1$, $8n+3$ der Reihe (1), sowie alle Primzahlen $8n+5$, $8n+7$ der Reihe (2) Divisoren, dagegen alle Primzahlen der Formen $8n+1$, $8n+3$ der Reihe (2) und alle Primzahlen $8n+5$, $8n+7$ der Reihe (1) Nichtdivisoren von $x^2 - a$.

Auch hier lassen sich beide Bedingungen, denen die Divisoren, wie auch die Nichtdivisoren zu genügen haben, in eine einzige vereinigen.

Beispiel. Es sollen die Divisoren von $x^2 - 10$ gefunden werden. Die Formen der Divisoren von $x^2 - 5$ sind

$$(1) \qquad 5k+1,\quad 5k+4,$$

die der Nichtdivisoren

$$(2) \qquad 5k+2,\quad 5k+3.$$

Divisoren von $x^2 - 10$ sind also alle Primzahlen $8n+1$, $8n+7$ der Reihe (1), das sind alle Primzahlen der Formen

$$40k+1,\quad 40k+9,\quad 40k+31,\quad 40k+39,$$

und ferner alle Primzahlen $8n+3$, $8n+5$ der Reihe (2), das sind alle Primzahlen der Formen

$$40k+3,\quad 40k+13,\quad 40k+27,\quad 40k+37.$$

Ebenso ergeben sich als Formen der Nichtdivisoren von x^2-10 zunächst

$$40k+11,\quad 40k+19,\quad 40k+21,\quad 40k+29$$

[das sind die Zahlen $8n+3$, $8n+5$ von (1)] und weiter

$$40k+7,\quad 40k+17,\quad 40k+23,\quad 40k+33$$

[Zahlen $8n+1$, $8n+7$ der Reihe (2)].

Aufgabe. Die Formen der Divisoren von x^2-77 zu ermitteln.

7 hat die Nichtreste 3, 10, 17, ...; 5, 12, 19, ...; 6, 13, 20, ...

11 hat die Nichtreste 2, 13, 24, ...; 6, 17, [28], ...; [7], 18, 29, ...; 8, 19, 30, ...; 10, [21], 32, ...

Nichtreste beider Zahlen oder keiner derselben sind

1, 4, 6, 9, 10, 13, 15, 16, 17, 19,
23, 24, 25, 36, 37, 40, 41, 52, 53, 54,
58, 60, 61, 62, 64, 67, 68, 71, 73, 76,

und es ergeben sich, wenn noch die Bedingung $p=2n+1$ zum Ausdruck gebracht wird, als Formen der Divisoren

$154k+$ 1, 9, 13, 15, 17, 19, 23, 25, 37, 41,
53, 61, 67, 71, 73, 81, 83, 87, 93, 101,
113, 117, 129, 131, 135, 137, 139, 141, 145, 153.

§ 95. Lösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten in rationalen Zahlen (Lagrange, Zusatz V zu Euler's Algebra). — Die Gleichung

$$(1)\qquad a+bx+cy+dx^2+exy+fy^2=0$$

oder

$$f^2y^2+(ex+c)fy=-f(a+bx+dx^2)$$

liefert

$$fy=-\frac{ex+c}{2}+\tfrac{1}{2}\sqrt{(ex+c)^2-4f(a+bx+dx^2)},$$

woraus

$$2fy+ex+c=\sqrt{x^2(e^2-4df)+2x(ec-2bf)+(c^2-4af)}$$

oder, wenn

$$c^2 - 4df = \gamma, \quad 2(ce - 2bf) = \beta, \quad e^2 - 4af = \alpha$$

gesetzt wird,

(2) $$2fy + ex + c = \sqrt{\alpha + \beta x + \gamma x^2}$$

folgt. Die Gleichung (1) durch rationale Werthe von x, y lösen heisst also diejenigen Werthe von x bestimmen (wenn es deren giebt), für welche $\alpha + \beta x + \gamma x^2$ ein vollständiges Quadrat wird, eine Aufgabe, die für 4 specielle Fälle schon § 28 behandelt worden ist und jetzt allgemein gelöst werden soll.

Wir beschäftigen uns also mit dem Ausdruck

(3) $$\sqrt{\alpha + \beta x + \gamma x^2} = z;$$

darin dürfen α, β, γ als ganze Zahlen vorausgesetzt werden; denn im entgegengesetzten Falle könnten wir sie unter einen und denselben Nenner N^2 bringen und diesen Nenner sodann unterdrücken. So ist z. B.

$$\sqrt{3 + \frac{5x}{4} - \frac{7x^2}{10}} = \frac{1}{10}\sqrt{300 + 125x - 70x^2};$$

$\sqrt{3 + \frac{5x}{4} - \frac{7x^2}{10}}$ wird also für dieselben Werthe von x rational werden, für welche $300 + 125x - 70x^2$ ein vollständiges Quadrat wird.

Aus (3) ergiebt sich

$$\gamma x^2 + \beta x = z^2 - \alpha,$$

also ist

$$x = \frac{1}{2\gamma}\left(-\beta + \sqrt{4\gamma z^2 + \beta^2 - 4\alpha\gamma}\right)$$

oder

(4) $$2\gamma x + \beta = \sqrt{4\gamma z^2 + (\beta^2 - 4\alpha\gamma)}.$$

Die Aufgabe ist somit darauf zurückgeführt,

$$\sqrt{4\gamma z^2 + (\beta^2 - 4\alpha\gamma)},$$

d. h. einen Ausdruck von der Form $\sqrt{Az^2 + B}$, in welchem A, B irgend welche gegebene positive oder negative ganze Zahlen sind, rational zu machen.

Dabei dürfen wir voraussetzen, dass weder A, noch B durch eine Quadratzahl theilbar sei. Wäre nämlich

$$A = a^2 A', \quad B = b^2 B',$$

so wäre

$$Az^2 + B = A'a^2z^2 + b^2B' = b^2\left(A'\frac{a^2z^2}{b^2} + B'\right)$$

oder, wenn

$$\frac{az}{b} = z'$$

gesetzt wird,

$$Az^2 + B = b^2(A'z'^2 + B'),$$

und sobald man die Werthe von z' gefunden hat, für welche $\sqrt{A'z'^2 + B'}$ rational ist, hat man auch die Werthe von $z = \frac{bz'}{a}$, welche $Az^2 + B$ zu einem Quadrat machen.

Wir betrachten also den Ausdruck $Az^2 + B$, in welcher A, B gegebene ganze Zahlen sind, die keine Quadratzahl als Divisor enthalten. z soll eine rationale Zahl sein. Wir setzen daher

$$z = \frac{p}{q}$$

und nehmen an, dass p prim zu q sei. Dann ist

$$A\frac{p^2}{q^2} + B$$

in ein Quadrat zu verwandeln. Es muss also auch

$$Ap^2 + Bq^2$$

ein Quadrat sein, d. h. wir haben die Gleichung

$$Ap^2 + Bq^2 = r^2, \tag{5}$$

in welcher A, B gegebene ganze Zahlen sind, in ganzen Werthen der drei Unbekannten p, q, r zu lösen.

Nun lässt sich leicht einsehen, dass A prim zu q sein muss. Hätten nämlich A und q einen gemeinschaftlichen Divisor $\delta > 1$, so wäre Bq^2 durch δ^2, aber Ap^2 nur durch δ theilbar; denn A enthält keine Quadratzahl als Divisor, und p ist prim zu q; daher würde

$$r^2 = Ap^2 + Bq^2$$

nur die erste Potenz von δ enthalten, könnte also kein Quadrat sein. Es ist demnach A prim zu q, und auf dieselbe Weise erkennt man, dass B prim zu p sein wird.

Nach diesen Vorbemerkungen gehen wir an die Auflösung der Gleichung (5).

Wir setzen $A > B$ voraus und schreiben die Gleichung in der Form

$$Ap^2 = r^2 - Bq^2. \tag{6}$$

Da A prim zu q ist, so lassen sich zwei ganze Zahlen n, q' ermitteln, welche der Gleichung

$$r = nq - Aq'$$

genügen. Indem wir unter n, q' vorläufig unbestimmte ganze Zahlen verstehen, setzen wir diesen Werth für r in (6) ein und erhalten nach leichten Reductionen

$$p^2 = \frac{n^2 - B}{A} q^2 - 2nqq' + Aq'^2,$$

woraus hervorgeht, dass die Gleichung (6) nur dann in ganzen Zahlen lösbar ist, wenn A in $n^2 - B$ aufgeht, wenn also B quadratischer Rest von A ist.

Wenn diese Bedingung erfüllt ist, so können wir n durch die absolut kleinste Wurzel der Congruenz

$$n^2 \equiv B \pmod{A}$$

ersetzen (diese Wurzel wird nicht $> \frac{A}{2}$ sein) und den Werth A' des Ausdrucks $\frac{n^2 - B}{A}$ bestimmen, wodurch wir die Gleichung

$$p^2 = A'q^2 - 2nqq' + Aq'^2 \tag{7}$$

erhalten, in welcher offenbar $A' < A$ ist.

Wenn jetzt A' eine Quadratzahl ist, so ist diese Gleichung auf die in § 28 dargelegte Weise zu behandeln, und man erhält die einfachste Lösung, wenn man

$$q' = 0, \quad q = 1, \quad p = \sqrt{A'}$$

macht.

Wenn A' keine Quadratzahl ist, aber einen quadratischen Factor enthält, so kann dieser auf die oben besprochene Art beseitigt werden. Wir nehmen an, dies sei eventuell geschehen, A' also durch kein Quadrat theilbar. Wenn dann $A' < B$ ist, so multipliciren wir (7) mit A' und erhalten

$$\begin{aligned} A'p^2 &= A'^2q^2 - 2A'nqq' + AA'q'^2 \\ &= (A'q - nq')^2 + q'^2(AA' - n^2) \end{aligned}$$

oder, da $AA' - n^2 = -B$ ist,

$$A'p^2 = (A'q - nq')^2 - Bq'^2,$$

und die Aufgabe ist darauf zurückgeführt, $A'p^2 + Bq'^2$ in ein Quadrat zu verwandeln, also eine Gleichung in ganzen Zahlen zu lösen, welche dieselbe Form wie (5), aber kleinere Coefficienten wie diese hat.

Wenn dagegen A' auch nach Unterdrückung eines etwa vorhandenen quadratischen Factors nicht $< B$ ist, so setzen wir in (7)

$$q = \nu q' + q'',$$

wo ν, q'' unbestimmte Zahlen bedeuten sollen. Dadurch geht (7) über in

$$\begin{aligned} p^2 &= A'(\nu q' + q'')^2 - 2nq'(\nu q' + q'') + Aq'^2 \\ &= A'q''^2 + (A'\nu^2 - 2n\nu + A)q'^2 - 2(n - A'\nu)q'q'' \end{aligned}$$

oder, wenn

$$\begin{aligned} A'\nu^2 - 2n\nu + A &= A'', \\ n - A'\nu \quad &= n' \end{aligned}$$

gesetzt wird, in

$$p^2 = A'q''^2 + A''q'^2 - 2n'q'q''. \tag{8}$$

Nun folgt aus der Definition von n'

$$n^2 - 2A'n\nu + A'^2\nu^2 = n'^2,$$

$$A'\nu^2 - 2n\nu = \frac{n'^2 - n^2}{A'},$$

also ist

$$A'' = \frac{n'^2 - n^2}{A'} + A = \frac{n'^2 - n^2 + AA'}{A'}$$

oder, weil $AA' = n^2 - B$ ist,

$$A'' = \frac{n'^2 - B}{A'}$$

und

$$p^2 = A'q''^2 + \frac{n'^2 - B}{A'}q'^2 - 2n'q'q''. \tag{9}$$

Daraus ergiebt sich, dass B quadratischer Rest von A' sein muss, wenn die Aufgabe lösbar sein soll, und es lässt sich für n' eine Zahl $< \frac{1}{2}A'$ bestimmen [eine Wurzel der Congruenz $n'^2 \equiv B \pmod{A'}$], durch deren Einsetzung

$$A'' = \frac{n'^2 - B}{A'} < A'$$

wird.

Mit der Gleichung (8) verfahren wir ganz so, wie wir mit (7) verfuhren.

Wir erhalten dadurch eine Zahl $A''' = \frac{a''^2 - B}{A''}$, weiter eventuell $A^{IV} = \frac{a'''^2 - B}{A'''}$, u. s. w., und da die Zahlen $A, A', A'', A''', \ldots$ eine abnehmende Reihe bilden, so werden wir endlich zu einer Zahl gelangen, welche kleiner als B ist. Dann führt uns aber das Verfahren, dem wir unter dieser Voraussetzung die Gleichung (7) unterzogen haben, zu einer Gleichung, welche die Form von (5), aber kleinere Coefficienten als diese hat.

Indem wir diese Gleichung in derselben Weise wie (5) behandeln, kommen wir zu einer Gleichung mit noch kleineren Coefficienten, und so werden wir schliesslich, wenn die vorgelegte Gleichung überhaupt in rationalen Zahlen lösbar ist, zu einer Gleichung gelangen, in welcher einer der Coefficienten A eine Quadratzahl ist. Nach Auflösung dieser Gleichung ermitteln wir rückwärts schreitend die Werthe, welche der vorgelegten Gleichung genügen.

Beispiel. Die Gleichung

$$(1) \qquad 6y^2 + 4xy - 28x^2 - 10y - 23 = 0$$

liefert, mit 6 multiplicirt und für $6y$ aufgelöst,

$$(2) \qquad 6y + 2x - 5 = \sqrt{172x^2 - 20x + 163}\,.$$

Wir setzen also

$$(3) \qquad \sqrt{172x^2 - 20x + 163} = z$$

und erhalten leicht

$$(4) \qquad 86x - 5 = \sqrt{43z^2 - 6984}\,.$$

Da $6984 = 2^3 \,.\, 3^2 \,.\, 97$, also durch 6^2 theilbar ist, so schreiben wir

$$(4^*) \qquad 86x - 5 = 6\sqrt{43\left(\frac{z}{6}\right)^2 - 194}\,,$$

haben also, wenn $\frac{z}{6} = z'$ gesetzt wird, $43z'^2 - 194$ in ein Quadrat zu verwandeln oder, wenn $z' = \frac{q}{p}$ gesetzt und unter z'' eine neue Unbekannte verstanden wird, die Gleichung

$$(5) \qquad 43q^2 - 194p^2 = z''^2$$

oder

$$(6) \qquad -194p^2 = z''^2 - 43q^2$$

in ganzen Zahlen zu lösen.

Wird hierin

$$z'' = nq - 194q'$$

gesetzt, so erhält man leicht

$$p^2 = \frac{q^2(n^2 - 43)}{-194} + 2nqq' - 194q'^2.$$

Nun hat die Congruenz

$$n^2 \equiv 43 \pmod{194}$$

die Wurzeln ± 25. Wir nehmen $n = 25$ an; dann ergiebt sich

$$\frac{n^2 - 43}{-194} = -3$$

und

$$p^2 = -3q^2 + 50qq' - 194q'^2.$$

Da $3 < 43$ ist, so multipliciren wir diese Gleichung mit -3 und erhalten

$$-3p^2 = 9q^2 - 150qq' + 582q'^2 = (3q - 25q')^2 - 43q'^2.$$

Die Aufgabe ist also darauf zurückgeführt, $43q'^2 - 3p^2$ in ein Quadrat zu verwandeln. Zu diesem Zwecke schreiben wir

$$(6^*) \qquad 43q'^2 = 3p^2 + z'''^2$$

und setzen hierin

$$z''' = n'p - 43q'',$$

wodurch wir

$$q'^2 = \frac{n'^2 + 3}{43} p^2 - 2n'pq'' + 43q''^2$$

erhalten. Die Congruenz

$$n'^2 \equiv -3 \pmod{43}$$

hat die Wurzeln ± 13. Für $n' = 13$ ist $\frac{n'^2 + 3}{43} = 4$, also

$$q'^2 = 4p^2 - 26pq'' + 43q''^2.$$

Jetzt ist der Coefficient von p^2 eine Quadratzahl. Wir setzen also

$$4p^2 - 26pq'' + 43q''^2 = (2p + rq'')^2$$

und erhalten

$$q'' = \frac{2p(2r + 13)}{43 - r^2},$$

wo für r und p beliebige rationale Werthe gesetzt werden können. Nachdem q'' bestimmt ist, erhält man rückwärts schreitend

$$q', z''', q, z', z, x, y.$$

Wird etwa $r = -7$, $p = 3$ angenommen, so ergiebt sich

$$q'' = 1,\ q' = 1,\ z''' = -4,\ q = 7,$$
$$z' = \tfrac{7}{3},\quad z = 14,\quad x = \tfrac{1}{2},\quad y = 3.$$

Hat man auf diese Weise einen einzigen Werth von x ermittelt, welcher den Ausdruck

$$\sqrt{\alpha + \beta x + \gamma x^2}$$

rational macht, so ist es leicht, eine Formel zu bilden, welche alle überhaupt möglichen Werthe von x, die dieses leisten, enthält. Ist nämlich

$$\alpha + \beta f + \gamma f^2 = g^2,$$

also

$$\alpha = g^2 - \beta f - \gamma f^2,$$

so ist

$$\alpha + \beta x + \gamma x^2 = g^2 + \beta(x - f) + \gamma(x^2 - f^2).$$

Dieser Ausdruck soll ein vollständiges Quadrat werden. Wir setzen daher

$$g^2 + \beta(x - f) + \gamma(x^2 - f^2) = [g + (x - f)m]^2,$$

wo m unbestimmt bleibt. Hieraus folgt, wenn man beiderseits g^2 subtrahirt und darauf durch $x - f$ dividirt,

$$\beta + \gamma(x + f) = 2gm + (x - f)m^2,$$

also

$$x = \frac{m^2 f - 2gm + \beta + \gamma f}{m^2 - \gamma},$$

und wegen der Unbestimmtheit von m muss dieser Ausdruck von x alle Werthe enthalten, die den vorgelegten Ausdruck

$$\alpha + \beta x + \gamma x^2$$

zu einem Quadrat machen.

So fanden wir oben, dass $\sqrt{172x^2 - 20x + 163}$ für $x = \frac{1}{2}$ rational, nämlich $= 14$ wird; hier ist

$$\beta = -20,\ \gamma = 172,\ f = \tfrac{1}{2},\ g = 14,$$

also

$$x = \frac{\frac{1}{2}m^2 - 28m + 66}{m^2 - 172}$$

der allgemeine Ausdruck der gesuchten Werthe von x.

§ 96. Vermischte Aufgaben.

1. Die Congruenz $13x^2 - 27x - 4 \equiv 0 \pmod{31}$ zu lösen.

Die Hülfscongruenz $13\alpha \equiv 1 \pmod{31}$ hat die Wurzel

$$\alpha \equiv 12 \pmod{31},$$

und durch Multiplication mit 12 geht die vorgelegte Congruenz über in

$$x^2 - 14x - 48 \equiv 0 \pmod{31};$$

es ist also

$$(x - 7)^2 \equiv 97 \equiv 4 \pmod{31},$$

$$x - 7 \equiv \pm 2 \pmod{31},$$

$$x_1 \equiv 9, \quad x_2 \equiv 5 \pmod{31}.$$

2. Es sind die Wurzeln ± 5 der Congruenz

$$x^2 \equiv 6 \pmod{19}$$

gegeben. Man soll die Congruenz $x^2 \equiv 6 \pmod{19^3}$ lösen.

Aus

$$(\pm 5 + 19y)^2 \equiv 6 \pmod{19^2}$$

folgt zunächst

$$\pm 190y \equiv -19 \pmod{19^2},$$

$$\pm 10y \equiv -1 \pmod{19},$$

$$\pm 10y \equiv 18 \pmod{19},$$

$$\pm 5y \equiv 9 \equiv -10 \pmod{19},$$

$$y \equiv \mp 2 \pmod{19},$$

$$x \equiv \pm 5 \mp 38 \equiv \mp 33 \pmod{19^2}.$$

Also hat die Congruenz

$$x^2 \equiv 6 \pmod{19^2}$$

die beiden Wurzeln

$$x \equiv \pm 33 \pmod{19^2}.$$

Wir setzen demnach weiter

$$x = \pm 33 + 19^2 y_1$$

und erhalten aus

$$(\pm 33 + 19^2 y_1)^2 \equiv 6 \pmod{19^3}$$

leicht

$$\pm 66 y_1 \equiv -3 \pmod{19},$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$y_1 \equiv \pm 6 \pmod{19}$$

und endlich

$$x \equiv \pm 33 \pm 6 \cdot 361 \equiv \pm 2199 \pmod{19^3}$$

als Wurzeln der Congruenz $x^2 \equiv 6 \pmod{19^3}$.

3. Die Congruenz $x^2 \equiv 25 \pmod{64}$ zu lösen.

Die Congruenz $x^2 \equiv 25$ hat

für den Modul 8 die Wurzeln ± 1, ± 3,
„ „ „ 16 „ „ ± 3, ± 5,
„ „ „ 32 „ „ ± 5, ± 11,
„ „ „ 64 „ „ ± 5, ± 27.

4. Die Primzahl 641 in 2 Quadrate zu zerlegen.

Die Congruenz $x^2 \equiv -1 \pmod{641}$ hat die Wurzeln ± 154.

$$\frac{641}{154} = 4 + \cfrac{1}{6 + \cfrac{1}{6 + \cfrac{1}{4}}}.$$

Näherungsbrüche:	4	6	
	$\frac{1}{0}$	$\frac{4}{1}$	$\frac{25}{6}$

Zerlegung: $641 = 25^2 + 4^2$.

5. Welche Wurzeln haben die Congruenzen:

1. $x^2 \equiv 35 \pmod{59}$ [± 25]
2. $x^2 \equiv 27 \pmod{37}$ [± 8]
3. $x^2 \equiv 46 \pmod{53}$ [± 24]
5. $x^2 \equiv 2 \pmod{97}$ [± 14]
6. $x^2 \equiv 3 \pmod{83}$ [± 13]
7. $x^2 \equiv 580 \pmod{5349 = 3 \,.\, 1783}$ [± 77, ± 1706].

6. Die Gleichung

$$9x^2 - 20xy - 5y^2 + 6x + 13y + 78 = 0$$

in rationalen Zahlen zu lösen.

Man erhält leicht

$$9x - 10y + 3 = \sqrt{145y^2 - 177y - 693},$$

und wenn

$$\sqrt{145y^2 - 177y - 693} = z$$

gesetzt wird,

$$290y - 177 = \sqrt{580z^2 + 433269}.$$

Da $433269 = 81 \,.\, 5349$ ist, so ist

$$290y - 177 = 9\sqrt{580z'^2 + 5349},$$

wo $z' = \frac{z}{9}$ ist.

Setzt man $z' = \frac{p}{q}$ und $\sqrt{580p^2 + 5349q^2} = z''$,
so ist

$$5349q^2 = z''^2 - 580p^2$$

oder, wenn

$$z'' = np - 5349q'$$

gesetzt wird,

$$q^2 = \frac{(n^2 - 580)p^2}{5349} - 2npq' + 5349q'^2.$$

Nun hat die Congruenz

$$n^2 \equiv 580 \pmod{5349}$$

die 4 Wurzeln ± 77, ± 1706. Wir nehmen $n = +77$ an und erhalten

$$q^2 = p^2 - 154pq' + 5349q'^2.$$

Wird jetzt

$$p^2 - 154pq' + 5349q'^2 = (p - rq')^2$$

gesetzt, so folgt leicht

$$q' = \frac{2p(77 - r)}{5349 - r^2}.$$

r und p sind unbestimmt, d. h. können beliebige rationale Zahlen sein. Ist q' bestimmt, so erhält man rückwärts schreitend die Werthe von q, z'', z', z, y, x.

Für $q = p - rq'$ ergiebt sich durch Einsetzung des Werthes von q'

$$q = \frac{5349p + pr^2 - 154pr}{5349 - r^2};$$

es ist also

$$z' = \frac{p}{q} = \frac{5349 - r^2}{5349 + r^2 - 154r},$$

mithin für $r = 0$

$$z' = 1, \quad z = 9, \quad y = 3, \quad x = 4.$$

Ueberhaupt wird

$$\sqrt{145y^2 - 177y - 693}$$

rational für jeden Werth

$$y = 3 \cdot \frac{m^2 - 6m + 86}{m^2 - 145},$$

wo m eine beliebige rationale Zahl ist. Für $m = 12$ ergiebt sich z. B. $y = -474$, $x = 582$.

Achtes Kapitel.

Allgemeine Sätze über binäre quadratische Formen und die Darstellung der Zahlen durch dieselben.

§ 97. Definition und Eintheilung der Formen. Determinante einer Form. — Wir haben uns jetzt noch mit der Auflösung der unbestimmten Gleichung zweiten Grades mit zwei Unbekannten in ganzen Zahlen zu beschäftigen. Diese Auflösung erfordert eine eingehende Betrachtung der binären quadratischen Formen, zu der wir unter Führung von Gauss, des Begründers dieser Theorie, uns jetzt wenden.

Eine ganze homogene Function von Veränderlichen, deren Coefficienten ganze Zahlen sind, wird in der Zahlentheorie eine Form genannt. Die Formen werden nach ihrem Grade in lineare, quadratische, cubische, u. s. w., und nach der Zahl der Veränderlichen, die sie enthalten, in binäre, ternäre, u. s. w. eingetheilt. Wir haben es in der Folge nur mit der binären quadratischen Form

$$ax^2 + 2bxy + cy^2$$

zu thun, in welcher a, b, c gegebene ganze Zahlen, x, y unbestimmte ganze Zahlen bezeichnen sollen. Den Coefficienten des mittleren Gliedes setzen wir immer als eine gerade Zahl voraus; falls derselbe ungerade sein sollte, multipliciren wir, um ihn gerade zu machen, die ganze Form mit 2.

Wenn es sich nicht um die Grössen x, y, sondern nur um die Coefficienten a, $2b$, c handelt, werden wir die Form kurz mit (a, b, c) bezeichnen. Da bei den Formen die Ordnung der Coefficienten von Bedeutung ist, so sind (a, b, c) und (c, b, a) wohl von einander zu unterscheiden.

Die Formen $x^2 + y^2$, $x^2 - 2y^2$, $3x^2 - 10xy - 5y^2$ werden also beziehungsweise durch $(1, 0, 1)$, $(1, 0, -2)$, $(3, -5, -5)$ bezeichnet werden.

Den Ausdruck $b^2 - ac$, von dessen Werthe, wie wir sehen werden, die Eigenschaften der Form

$$(a,\ b,\ c) = ax^2 + 2bxy + cy^2$$

in hohem Grade abhängen, nennt man die **Determinante** dieser Form. Die Determinanten der Formen

$$(3,\ 4,\ 7),\ (1,\ -1,\ 1),\ (0,\ 3,\ a)$$

sind also beziehungsweise -5, 0, 9.

Die Determinante einer Form ist positiv, Null oder negativ. Da die Formen, deren Determinante Null ist, eine eigene Behandlung erfordern, so schliessen wir sie vorläufig von der Betrachtung vollständig aus.

§ 98. Transformation der Formen. — Wenn wir in einer Form

$$F = ax^2 + 2bxy + cy^2 \tag{1}$$

die Grössen x, y durch die Ausdrücke

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases} \tag{2}$$

ersetzen, wo α, β, γ, δ ganze Zahlen sind, so verwandelt sich F in die neue Form

$$F' = a'x'^2 + 2b'x'y' + c'y'^2, \tag{3}$$

und es ist, wie eine leichte Rechnung ergiebt,

$$\begin{cases} a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' = a\beta^2 + 2b\beta\delta + c\delta^2. \end{cases} \tag{4}$$

Man sagt dann, man habe die Form F vermittels der **Substitution** (2) in die Form F' transformirt.

Wenn die Form F' einen Werth M annimmt, sobald $x' = m$, $y' = n$ gesetzt wird, so wird auch die Form F gleich M werden, wenn man $x = \alpha m + \beta n$, $y = \gamma m + \delta n$ setzt. Daher wird jede durch F' darstellbare Zahl sich auch durch F darstellen lassen, oder alle durch F' darstellbaren Zahlen werden unter den durch F darstellbaren enthalten sein. Man sagt daher, die Form F' sei **unter** F **enthalten**, oder F **enthalte** F'.

Die aus den Coefficienten der Substitution (2) gebildete Zahl

$$\alpha\delta - \beta\gamma$$

nennt man die Determinante der Substitution.

Die Determinante einer Substitution kann eine positive oder eine negative Zahl sein. Im ersteren Falle nennt man die Substitution eine eigentliche und sagt, die Form F' sei unter F eigentlich enthalten. Im zweiten Falle heisst die Substitution eine uneigentliche und F' unter F uneigentlich enthalten.

Da eine Form F in eine andere F' möglicherweise durch verschiedene Substitutionen übergeführt werden kann, die zum Theil eigentliche, zum Theil uneigentliche sein können, so ist es auch recht wohl möglich (wir werden solche Fälle weiterhin wirklich antreffen), dass eine Form F' unter einer andern Form F eigentlich und zugleich uneigentlich enthalten sei.

Zwei oder mehrere Substitutionen heissen gleichartig, wenn sie sämmtlich eigentliche, oder sämmtlich uneigentliche sind. Im entgegengesetzten Falle werden sie ungleichartig genannt.

Lehrsatz. Die Determinante einer Form F', welche durch eine beliebige Substitution aus einer Form F entstanden ist, ist gleich dem Produkt aus der Determinante der letzteren in das Quadrat der Determinante der Substitution.

Beweis. Bildet man mittels der Formeln (4) den Ausdruck $b'^2 - a'c'$, so erhält man nach einigen leichten Reductionen

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2 .$$

Diese Formel beweist nicht nur den in Rede stehenden Satz, sondern lässt zugleich erkennen, dass die Determinanten beider Formen dasselbe Vorzeichen haben.

Aufgabe. Eine Form $F = (a, b, c)$ ist durch eine Substitution

$$(1) \qquad \begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases}$$

in $F' = (a', b', c')$ transformirt worden. Man soll die Substitution ermitteln, welche umgekehrt F' wieder in F verwandelt.

Lösung. Es sei

$$\begin{cases} x' = \alpha' x + \beta' y \\ y' = \gamma' x + \delta' y \end{cases}$$

die gesuchte Substitution, so wird F offenbar in sich selbst transformirt, d. h. unverändert bleiben, wenn man

$$x = \alpha(\alpha' x + \beta' y) + \beta(\gamma' x + \delta' y),$$
$$y = \gamma(\alpha' x + \beta' y) + \delta(\gamma' x + \delta' y)$$

oder

$$x = (\alpha\alpha' + \beta\gamma')x + (\alpha\beta' + \beta\delta')y,$$
$$y = (\gamma\alpha' + \delta\gamma')x + (\gamma\beta' + \delta\delta')y$$

setzt. Es muss somit

$$\alpha\alpha' + \beta\gamma' = 1,$$
$$\alpha\beta' + \beta\delta' = 0,$$
$$\gamma\alpha' + \delta\gamma' = 0,$$
$$\gamma\beta' + \delta\delta' = 1$$

sein, und hieraus ergiebt sich leicht, wenn die Determinante der Substitution (1) der Kürze wegen mit ε bezeichnet wird,

$$\alpha' = \frac{\delta}{\varepsilon}, \quad \beta' = -\frac{\beta}{\varepsilon}, \quad \gamma' = -\frac{\gamma}{\varepsilon}, \quad \delta' = \frac{\alpha}{\varepsilon}.$$

Diese Werthe von α', β', γ', δ' sind nur dann ganze Zahlen, wenn $\varepsilon = +1$ oder $= -1$ ist. Wir schliessen daraus Folgendes: Wenn die Form F durch die Substitution (1) in F' transformirt ist, so lässt sich nicht immer auch F' zurück in F transformiren. Dies ist vielmehr nur möglich, wenn die Determinante der Substitution den Werth ± 1 hat, und dann verwandelt sich F' in F, wenn man

$$(2) \qquad \begin{cases} x' = \varepsilon\delta x - \varepsilon\beta y \\ y' = -\varepsilon\gamma x + \varepsilon\alpha y \end{cases}$$

setzt, wo $\varepsilon = \pm 1$ die Determinante $\alpha\delta - \beta\gamma$ der Substitution (1) ist.

Beispiel. Die Form $x^2 + 8xy - y^2 = (1, 4, -1)$ geht durch die Substitution

$$\begin{cases} x = x' - 2y' \\ y = 2x' - 3y', \end{cases}$$

deren Determinante $+1$ ist, über in

$$13x'^2 - 48x'y' + 43y'^2 = (13, -24, 43),$$

und letztere wird wieder in $(1, 4, -1)$ transformirt, wenn man

$$x' = -3x + 2y,$$
$$y' = -2x + y$$

setzt.

§ 99. Aequivalente Formen. — Zwei Formen F, F' von der Beschaffenheit, dass F' unter F und zugleich F unter F' enthalten sei, heissen äquivalent. Damit F und F' äquivalent seien, sind also, wie die Lösung der vorhergehenden Aufgabe ergiebt, zwei Bedingungen zu erfüllen, nämlich 1), dass F' unter F enthalten sei, und 2), dass die Determinante der Substitution, durch welche F in F' übergeht, den Werth ± 1 habe. Wenn die zweite Bedingung erfüllt ist, so lehrt der Satz des vorhergehenden Paragraphen, dass beide Formen die nämliche Determinante haben. Die Aequivalenz zweier Formen erfordert also die Gleichheit ihrer Determinanten; man darf aber, die erste Bedingung vernachlässigend, aus der Gleichheit der Determinanten allein durchaus nicht auf die Aequivalenz zweier Formen schliessen.

Wenn die Form F durch die Substitution

$$(1) \qquad \begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases}$$

in die äquivalente Form F' transformirt wird, so geht, wie wir gesehen haben, F' in F über durch die Substitution

$$(2) \qquad \begin{cases} x' = \quad \varepsilon\delta x - \varepsilon\beta y \\ y' = -\varepsilon\gamma x + \varepsilon\alpha y, \end{cases}$$

wo ε die Determinante von (1), also $\varepsilon^2 = +1$ ist. Die Substitution (2) hat daher dieselbe Determinante $\alpha\delta - \beta\gamma$ wie (1), und somit sind beide Substitutionen eigentliche oder beide uneigentliche. Im ersteren Falle heissen die Formen F, F' eigentlich äquivalent, im zweiten uneigentlich äquivalent.

Beispiele. I. Die Form $(5, 7, -1)$, deren Determinante 54 ist, geht durch die Substitution

$$x = 5x' + 2y', \qquad y = 7x' + 3y'$$

über in die Form $(566, 232, 95)$, welche dieselbe Determinante hat. Die letztere Form geht durch die Substitution

$$x' = 3x - 2y, \qquad y' = -7x + 5y$$

wieder in $(5, 7, -1)$ über. Beide Formen sind **eigentlich äquivalent**, da die Determinante jeder Substitution $+1$ ist.

II. Die Form $(3, -4, 4)$ mit der Determinante 4 geht durch die Substitution $x = x' + y', y = 2x' + y'$ in $(3, -1, -1)$ über. Die letztere Form, welche gleichfalls die Determinante 4 hat, wird durch die Substitution $x' = -x + y, y' = 2x - y$ wieder in $(3, -4, 4)$ transformirt. Da jede dieser beiden Substitutionen die Determinante -1 hat, so sind beide Formen **uneigentlich äquivalent**.

Die Formeln (4) des § 98, welche uns die Coefficienten a', b', c' der Form liefern, die durch irgend eine Substitution aus einer gegebenen Form (a, b, c) entsteht, lassen erkennen, dass jeder gemeinschaftliche Divisor der Zahlen a, b, c auch Divisor der Zahlen a', b', c' sein wird. Denkt man sich die zweite dieser Formeln (4) beiderseits mit 2 multiplicirt, so geht aus denselben ebenso hervor, dass jeder gemeinschaftliche Divisor der Zahlen $a, 2b, c$ auch Divisor der Zahlen $a', 2b', c'$ ist. Es wird mithin auch der **grösste gemeinschaftliche Divisor** der Zahlen a, b (resp. $2b$), c in a', b' (resp. $2b'$), c' aufgehen. Wenn nun beide Formen äquivalent sind, so muss der grösste gemeinschaftliche Divisor von a, b $(2b)$, c in den von a', b' $(2b')$, c' und zugleich der grösste gemeinschaftliche Divisor von a', b' $(2b')$, c' in den von a, b $(2b)$, c aufgehen, d. h. der grösste gemeinschaftliche Divisor von a, b $(2b)$, c **muss gleich demjenigen von a', b' $(2b')$, c' sein.**

Aufgabe. Es sollen die Beziehungen der beiden Formen (c, b, a) und $(a, -b, c)$ zu (a, b, c) ermittelt werden.

Lösung. (c, b, a) geht aus (a, b, c) durch Vertauschung von x und y, also durch die Substitution

$$\begin{cases} x = 0 \cdot x' + 1 \cdot y' \\ y = 1 \cdot x' + 0 \cdot y' \end{cases}$$

hervor; da die Determinante dieser Substitution -1 ist, so sind beide Formen uneigentlich äquivalent.

$(a, -b, c)$ geht aus (a, b, c) durch die Substitution

$$\begin{cases} x = 1 \cdot x' + 0 \cdot y' \\ y = 0 \cdot x' - 1 \cdot y' \end{cases}$$

hervor; diese hat die Determinante -1, also sind auch die

beiden Formen (a, b, c), $(a, -b, c)$, welche man entgegengesetzte nennt, uneigentlich äquivalent.

§ 100. Formen, von denen jede die folgende enthält. —

Lehrsatz I. Wenn eine Form F eine zweite F' und diese zweite eine dritte F'' enthält, so enthält auch die erste die dritte und zwar eigentlich oder uneigentlich, je nachdem die zweite Form die dritte in derselben Weise enthält, wie die erste die zweite, oder in entgegengesetzter Weise.

Beweis. Wenn F durch die Substitution

$$(1)\qquad \begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases}$$

in F' und F' durch die Substitution

$$(2)\qquad \begin{cases} x' = \alpha' x'' + \beta' y'' \\ y' = \gamma' x'' + \delta' y'' \end{cases}$$

in F'' übergeht, so wird sich F durch die Substitution

$$\begin{cases} x = \alpha\,(\alpha' x'' + \beta' y'') + \beta\,(\gamma' x'' + \delta' y'') \\ y = \gamma\,(\alpha' x'' + \beta' y'') + \delta\,(\gamma' x'' + \delta' y'') \end{cases}$$

oder, was dasselbe ist,

$$(3)\qquad \begin{cases} x = (\alpha\alpha' + \beta\gamma')\,x'' + (\alpha\beta' + \beta\delta')\,y'' \\ y = (\gamma\alpha' + \delta\gamma')\,x'' + (\gamma\beta' + \delta\delta')\,y'' \end{cases}$$

in F'' verwandeln. Somit enthält F auch F''.

Nun ergiebt sich durch Ausführung der Multiplicationen leicht, dass

$$\begin{aligned}(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma')\\ = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma'),\end{aligned}$$

dass also die Determinante der Substitution (3) das Produkt der Determinanten von (1) und (2) ist. F enthält somit F'' eigentlich oder uneigentlich, je nachdem die Substitutionen (1) und (2) gleichartig oder ungleichartig sind.

Zusatz. Wenn in einer beliebig grossen Reihe von Formen eine jede die folgende enthält, so wird auch die erste die letzte enthalten und zwar eigentlich oder uneigentlich, je nachdem die Anzahl der Formen,

welche die auf sie folgende Form uneigentlich enthalten, gerade oder ungerade ist.

Lehrsatz II. Wenn eine Form F einer zweiten F' und diese zweite einer dritten F'' äquivalent ist, so ist auch die erste der dritten äquivalent, und zwar eigentlich oder uneigentlich, je nachdem die zweite Form der dritten in derselben oder in entgegengesetzter Weise äquivalent ist, wie die erste der zweiten.

Beweis. Da F äquivalent F' und F' äquivalent F'' ist, so ist einerseits F unter F' und F' unter F'', also auch F unter F'', andererseits aber auch F'' unter F' und F' unter F, also auch F'' unter F enthalten. Somit sind die Formen F, F'' äquivalent.

Wenn nun die erste Form die zweite in derselben Weise enthält, wie die zweite die dritte, so enthält die erste Form die dritte eigentlich und ist zugleich unter derselben eigentlich enthalten; daher sind die Formen F, F'' in diesem Falle eigentlich, im entgegengesetzten Falle uneigentlich äquivalent.

§ 101. Benachbarte Formen. — Wenn zwei Formen (a, b, c) und (a', b', c') gleiche Determinanten haben, und wenn zugleich $a' = c$ und $b + b' \equiv 0 \pmod{c}$ ist, so nennt man die Formen benachbart, und zwar sagt man, wenn eine genauere Angabe erforderlich ist, (a, b, c) sei der Form (c, b', c') nach links benachbart oder (c, b', c') sei der Form (a, b, c) nach rechts benachbart. So ist z. B. $(9, 2, -11)$ der Form $(-11, 9, 2)$ nach links benachbart, $(3, 1, 3)$ ist $(3, -1, 3)$ sowohl nach links, als auch nach rechts benachbart.

Aufgabe I. Die Formen zu bestimmen, welche einer gegebenen Form (a, b, c) benachbart sind.

Lösung. Es seien a', b', c' die Coefficienten einer Form, die (a, b, c) nach rechts benachbart sein möge. Dann ist zunächst $a' = c$ und, weil $b' + b \equiv 0 \pmod{c}$ sein soll, $b' = -b + kc$, wo k eine unbestimmt bleibende ganze Zahl bezeichnet. Nun müssen beide Formen noch dieselbe Determinante haben; es muss also

$$(-b + kc)^2 - cc' = b^2 - ac$$

sein, und hieraus ergiebt sich leicht

$$c' = a - 2bk + ck^2.$$

Es ist also

$$(c, -b + kc, a - 2bk + ck^2)$$

der allgemeine Ausdruck der (a, b, c) nach rechts benachbarten Formen.

In derselben Weise würden wir als allgemeinen Ausdruck der (a, b, c) nach links benachbarten Formen

$$(c - 2bk + ak^2, -b + ka, a)$$

erhalten haben.

Lehrsatz. Zwei benachbarte Formen sind eigentlich äquivalent.

Beweis. Die Form (a, b, c) geht in

$$(c, -b + kc, a - 2bk + ck^2)$$

durch die Substitution

$$\begin{cases} x = 0 \cdot x' - 1 \cdot y' \\ y = 1 \cdot x' + k \cdot y' \end{cases}$$

über. Da die Determinante dieser Substitution den Werth $+1$ hat, so sind beide Formen eigentlich äquivalent.

Aufgabe II. Es ist eine Form (a, b, c) gegeben. Eine zweite Form soll mit der gegebenen den ersten Coefficienten a gemeinsam haben und derselben eigentlich äquivalent sein. Welches ist diese zweite Form?

Lösung. (a, b, c) ist uneigentlich äquivalent (c, b, a), (c, b, a) ist uneigentlich äquivalent $(c, -b, a)$, folglich ist (a, b, c) eigentlich äquivalent $(c, -b, a)$. Ferner ist $(c, -b, a)$ eigentlich äquivalent

$$(a, b + ak, c + 2bk + ak^2);$$

diese letztere Form ist also die gesuchte, und darin kann k jede ganze Zahl sein.

Aufgabe III. Zu beweisen, dass die Form (a, b, c), wenn $2b$ durch a theilbar ist, sich selbst uneigentlich äquivalent ist.

Unter der gemachten Voraussetzung ist (a, b, c), weil nach rechts benachbart, eigentlich äquivalent (c, b, a); (c, b, a) ist aber (a, b, c) uneigentlich äquivalent; folglich ist (a, b, c) sich selbst uneigentlich äquivalent.

Anmerkung. Es wird hier vorausgesetzt, dass der Coefficient, der in den benachbarten Formen derselbe ist, von Null verschieden sei. Dies ist übrigens immer der Fall, wofern nicht die Determinante der Form eine Quadratzahl ist.

Aufgabe IV. Zu beweisen, dass die Formen

$$(a, a+1, a+2) \quad \text{und} \quad (a+2, a+3, a+4),$$

für jeden Werth der ganzen Zahl a benachbart sind, und die Substitution zu ermitteln, durch welche die erste Form in die zweite transformirt wird.

Lösung. Da

$$(a+1)+(a+3)=2a+4$$

durch $a+2$ theilbar und zugleich

$$(a+1)^2-a(a+2)=(a+3)^2-(a+2)(a+4)$$

ist, so sind die Formen benachbart.

Nun geht allgemein eine Form (a, b, c) in die benachbarte $(c, -b+kc, a-2bk+ck^2)$ über, wenn man

$$x=0\cdot x'-1\cdot y',\ y=1\cdot x'+ky'$$

setzt; wir haben also, da hier $b=a+1$, $c=a+2$ ist, über k so zu verfügen, dass

$$k(a+2)-(a+1)=a+3$$

wird. Es ergiebt sich hieraus $k=2$; die gesuchte Substitution ist also

$$x=-y',\ y=x'+2y'.$$

§ 102. Zusammenhang zwischen zwei gleichartigen Transformationen einer Form in eine andere. — Es seien

$$F=ax^2+2bxy+cy^2 \quad \text{und} \quad F'=a'x'^2+2b'x'y'+c'y'^2$$

zwei gegebene Formen, deren Determinanten beziehungsweise d und d' sind, und es möge F in F' transformirt werden durch jede der beiden gleichartigen Substitutionen

$$\begin{cases} x=\alpha x'+\beta y' \\ y=\gamma x'+\delta y' \end{cases}, \quad \begin{cases} x=\alpha' x'+\beta' y' \\ y=\gamma' x'+\delta' y' \end{cases},$$

von denen die erstere die Determinante ε, die zweite die Determinante ε' habe.

Dann ist nach dem Lehrsatz des § 98

$$d' = d\varepsilon^2 \quad \text{und} \quad d' = d\varepsilon'^2,$$

also $\varepsilon^2 = \varepsilon'^2$ und, da beide Substitutionen gleichartig sein sollen, $\varepsilon = \varepsilon'$. Ferner bestehen nach § 98, (4) die 6 Gleichungen

(1) $$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$$

(2) $$a' = a\alpha'^2 + 2b\alpha'\gamma' + c\gamma'^2$$

(3) $$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta$$

(4) $$b' = a\alpha'\beta' + b(\alpha'\delta' + \beta'\gamma') + c\gamma'\delta'$$

(5) $$c' = a\beta^2 + 2b\beta\delta + c\delta^2$$

(6) $$c' = a\beta'^2 + 2b\beta'\delta' + c\delta'^2.$$

Wir setzen jetzt der Kürze wegen

$$a\alpha\alpha' + b(\alpha\gamma' + \gamma\alpha') + c\gamma\gamma' = A,$$

$$a(\alpha\beta' + \beta\alpha') + b(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + c(\gamma\delta' + \delta\gamma') = 2B,$$

$$a\beta\beta' + b(\beta\delta' + \delta\beta') + c\delta\delta' = C.$$

Nun ergiebt sich durch Multiplication von (1) und (2)

(7) $$a'^2 = A^2 - d(\alpha\gamma' - \gamma\alpha')^2.$$

Wenn wir weiter (1) mit (4), darauf (2) mit (3) multipliciren und die Produkte addiren [Um für die Folge eine kurze Ausdrucksweise zu gewinnen, werden wir dafür $(1)\cdot(4) + (2)\cdot(3)$ schreiben], so folgt

(8) $$2a'b' = 2AB - d(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha').$$

Durch $(1).(6) + (2).(5) + 2.(3).(4)$ ergiebt sich

$$2b'^2 + 2a'c' = 4B^2 - d[(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2\varepsilon\varepsilon'],$$

und hieraus folgt durch Addition von

$$2b'^2 - 2a'c' = 2d' = 2d\varepsilon\varepsilon'$$

(9) $$4b'^2 = 4B^2 - d(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2.$$

Weiter erhält man durch $(3).(4)$

$$b'^2 = AC - d(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha'),$$

und wenn hiervon

$$b'^2 - a'c' = d(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

subtrahirt wird, so folgt

(10) $$a'c' = AC - d(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta').$$

Durch (3) . (6) + (4) . (5) ergiebt sich

$$(11)\quad 2b'c' = 2BC - d(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta')$$

und durch (5) . (6)

$$(12)\qquad c'^2 = C^2 - d(\beta\delta' - \delta\beta')^2.$$

Wir nehmen jetzt an, der grösste gemeinschaftliche Divisor der Zahlen a', $2b'$, c' sei m, und wir hätten nach § 24, VI drei ganze Zahlen g, h, k bestimmt, welche der Gleichung

$$a'g + 2b'h + c'k = m$$

genügen. Wenn man dann die 6 Gleichungen (7)—(12) beziehungsweise mit g^2, $2gh$, h^2, $2gk$, $2hk$, k^2 multiplicirt und die Produkte addirt, so ergiebt sich

$$(Ag + 2Bh + Ck)^2$$
$$- d[g(\alpha\gamma' - \gamma\alpha') + h(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')$$
$$+ k(\beta\delta' - \delta\beta')]^2 = m^2,$$

oder, wenn der Kürze wegen

$$(13)\qquad Ag + 2Bh + Ck = T,$$

$$(14)\quad \begin{cases} g(\alpha\gamma' - \gamma\alpha') + h(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta') \\ \qquad + k(\beta\delta' - \delta\beta') = U \end{cases}$$

gesetzt wird,

$$T^2 - dU^2 = m^2.$$

Zwei gleichartige Transformationen einer Form F in F' liefern also eine ganzzahlige Lösung

$$t = T, \quad u = U$$

der Gleichung

$$t^2 - du^2 = m^2.$$

Beispiel. Die Form $x^2 + 3y^2$ wird in

$$16x'^2 + 72x'y' + 84y'^2$$

transformirt durch jede der beiden Substitutionen

$$\begin{cases} x = 2x' + 6y' \\ y = 2x' + 4y', \end{cases} \qquad \begin{cases} x = 4x' + 9y' \\ y = \qquad - y'. \end{cases}$$

Es ergiebt sich

$$A = 8, \quad 2B = 36, \quad C = 42, \quad d = -3, \quad m = 4,$$

und da die Gleichung

$$16g + 72h + 84k = 4$$

durch die Werthe $g = -8$, $h = -1$, $k = 5$ befriedigt wird, so liefern unsere beiden Substitutionen für die Gleichung

$$t^2 + 3u^2 = 16$$

die Lösung

$$t = 8 \,.\, (-8) + 36 \,.\, (-4) + 42 \,.\, 5 = +2$$
$$u = (-8) \,.\, (-8) - 4 \,.\, (-36) + 5 \,.\, (-42) = -2 \,.$$

In unseren Schlüssen ist nicht vorausgesetzt, dass die beiden Transformationen verschieden seien. Wir können dieselben also auch als identisch ansehen, d. h. $\alpha' = \alpha$, $\beta' = \beta$, $\gamma' = \gamma$, $\delta' = \delta$ setzen. Dann liefert die Gleichung (14) $U = 0$; ferner wird $A = a'$, $B = b'$, $C = c'$, folglich (wegen (13)) $t = m$. Wir erhalten also die Lösung $u = 0$, $t = \pm m$, die der blosse Anblick der Gleichung unmittelbar liefert.

Bekanntlich können die Zahlen g, h, k auf unendlich viele Arten bestimmt werden. Wir werden jetzt sehen, dass T und U von den für g, h, k gewählten Werthen ganz unabhängig sind. Zu diesem Zwecke wollen wir Formeln für T und U herleiten, die einfacher als (13) und (14) sind, also auch den Vortheil gewähren, schneller die Werthe von T und U zu liefern. Wir erhalten durch

$$(1).(\delta\alpha' - \beta\gamma') + (2).(\alpha\delta' - \gamma\beta') + (3).(\alpha\gamma' - \gamma\alpha') + (4).(\gamma\alpha' - \alpha\gamma')$$

$$(15)\quad \begin{cases} a'(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') \\ = A\,[(\alpha\delta - \beta\gamma) + (\alpha'\delta' - \beta'\gamma')] = A(\varepsilon + \varepsilon'), \end{cases}$$

ferner durch

$$[(1)-(2)].(\delta\beta' - \beta\delta') + [(3)+(4)].(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') + [(5)-(6)].(\alpha\gamma' - \gamma\alpha')$$

$$(16)\quad \begin{cases} 2b'(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') \\ = 2B(\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma') = 2B(\varepsilon + \varepsilon'), \end{cases}$$

endlich durch

$$[(3)-(4)].(\delta\beta' - \beta\delta') + (5).(\alpha\delta' - \gamma\beta') + (6).(\delta\alpha' - \beta\gamma')$$

$$(17)\quad \begin{cases} c'(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') \\ = C(\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma') = C(\varepsilon + \varepsilon'). \end{cases}$$

Da $\varepsilon = \varepsilon'$ ist, so folgt aus den Gleichungen (15), (16), (17)

$$A = \frac{a'(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')}{2\varepsilon},$$

$$2B = \frac{2b'(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')}{2\varepsilon},$$

$$C = \frac{c'(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')}{2\varepsilon},$$

und durch Einsetzung dieser Werthe geht (13) über in

$$(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')\frac{a'g + 2b'h + c'k}{2\varepsilon} = T$$

oder, da $a'g + 2b'h + c'k = m$ ist, in

$$(18) \qquad 2\varepsilon T = m(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha').$$

Dies ist die Formel, aus welcher sich T leicht berechnen lässt, und welche zeigt, dass der Werth von T von den Werthen, die wir für g, h, k wählen, ganz unabhängig ist.

Aus (18) ergiebt sich für $\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha'$ der Werth $\frac{2\varepsilon T}{m}$, durch dessen Einsetzung in (15), (16), (17) man

$$mA = Ta', \quad 2mB = 2Tb', \quad mC = Tc'$$

erhält, und bei Benutzung dieser Werthe von A, $2B$, C erhalten wir aus (7)–(12), wenn wir noch $m^2 + dU^2$ statt T^2 schreiben, nach leichten Vereinfachungen

$$(7*) \qquad a'^2 U^2 = (\alpha\gamma' - \gamma\alpha')^2 m^2$$

$$(8*) \qquad 2a'b'U^2 = (\alpha\gamma' - \gamma\alpha')(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')m^2$$

$$(9*) \qquad 4b'^2 U^2 = (\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')^2 m^2$$

$$(10*) \qquad a'c'U^2 = (\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')m^2$$

$$(11*) \qquad 2b'c'U^2 = (\beta\delta' - \delta\beta')(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')m^2$$

$$(12*) \qquad c'^2 U^2 = (\beta\delta' - \delta\beta')^2 m^2.$$

Hieraus ergiebt sich bei Benutzung der Gleichung (14) und der Gleichung

$$a'g + 2b'h + c'k = m$$

durch $(7*) . g + (8*) . h + (10*) . k$

$$a'mU^2 = (\alpha\gamma' - \gamma\alpha')m^2 U$$

oder

$$(19) \qquad a'U = (\alpha\gamma' - \gamma\alpha')m,$$

durch $(8*) . g + (9*) . h + (11*) . k$

$$2b'mU^2 = (\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')m^2 U$$

oder

$$(20) \qquad 2b'U = (\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')m,$$

endlich durch $(10*) . g + (11*) . h + (12*) . k$

$$c'mU^2 = (\beta\delta' - \delta\beta')m^2 U$$

oder

(21) $$c'U = (\beta\delta' - \delta\beta')\,m.$$

Jede dieser Formeln (19)—(21) zeigt, dass auch U von g, h, k unabhängig ist, und setzt uns in den Stand, U mit Leichtigkeit zu berechnen.

§ 103. Ermittlung der mit einer gegebenen Transformation gleichartigen Transformationen einer Form in eine andere. — Es seien wieder F, F' zwei gegebene Formen, und es gehe F in F' über durch die gegebene Substitution

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'.$$

Wir stellen uns die Aufgabe, alle mit der gegebenen gleichartigen Substitutionen zu ermitteln. Dabei setzen wir die Lösung T, U der Gleichung $t^2 - du^2 = m^2$, in welcher d, m die im vorigen Paragraphen festgesetzte Bedeutung haben, als bekannt voraus. Die gesuchte Substitution bezeichnen wir mit

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'.$$

Unsere Aufgabe läuft dann darauf hinaus, α', β', γ', δ' durch α, β, γ, δ, T, U auszudrücken, und dies geschieht auf folgende Weise:

Durch $(18).\alpha + (19).2\beta - (20).\alpha$ erhalten wir

$$2\alpha\varepsilon T + 2(\beta a' - \alpha b')U = 2(\alpha\delta - \beta\gamma)\,\alpha' m = 2\varepsilon\alpha' m,$$

ebenso durch $(18).\beta + (20).\beta - (21).2\alpha$

$$2\beta\varepsilon T + 2(\beta b' - \alpha c')U = 2(\alpha\delta - \beta\gamma)\beta' m = 2\varepsilon\beta' m,$$

ferner durch $(18).\gamma + (19).2\delta - (20).\gamma$

$$2\gamma\varepsilon T + 2(\delta a' - \gamma b')U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2\varepsilon\gamma' m,$$

endlich durch $(18).\delta + (20).\delta - (21).2\gamma$

$$2\delta\varepsilon T + 2(\delta b' - \gamma c')U = 2(\alpha\delta - \beta\gamma)\delta' m = 2\varepsilon\delta' m,$$

und wenn man in diese Formeln die Werthe von a', b', c' aus (1), (3), (5) einsetzt, so liefern dieselben

$$\alpha' = \frac{1}{m}\,[\alpha T - (b\alpha + c\gamma)\,U],$$

$$\beta' = \frac{1}{m}\,[\beta T - (b\beta + c\delta)\,U],$$

$$\gamma' = \frac{1}{m}\,[\gamma T + (a\alpha + b\gamma)\,U],$$

$$\delta' = \frac{1}{m}\,[\delta T + (a\beta + b\delta)\,U].$$

Wir sehen somit, dass jede mit der gegebenen gleichartige Substitution, durch welche F in F'' transformirt wird, in den Formeln

$$(22)\quad \begin{cases} x = \frac{1}{m}[\alpha T - (b\alpha + c\gamma)U]x' \\ \quad + \frac{1}{m}[\beta T - (b\beta + c\delta)U]y' \\ y = \frac{1}{m}[\gamma T + (a\alpha + b\gamma)U]x' \\ \quad + \frac{1}{m}[\delta T + (a\beta + b\delta)U]y' \end{cases}$$

enthalten ist.

Es bleibt nun noch zu zeigen, dass jede durch diese Formeln ausgedrückte Substitution wirklich F in F'' verwandelt und dabei mit der gegebenen gleichartig ist. Der erste Punkt wird dadurch bewiesen, dass man die in (22) angegebenen Werthe von x, y in

$$F = ax^2 + 2bxy + cy^2$$

einsetzt; unter Anwendung der Gleichung

$$T^2 - dU^2 = m^2$$

überzeugt man sich dann, freilich mittels mühseliger Rechnung, dass die Coefficienten von x'^2, $x'y'$, y'^2 in der That a', $2b'$, c' werden, dass also F in F'' transformirt wird.

Für die Determinante der Substitution (22) erhält man durch wirkliche Berechnung

$$\frac{1}{m^2}[T^2(\alpha\delta - \beta\gamma) - b^2U^2(\alpha\delta - \beta\gamma) + ac\,.\,U^2(\alpha\delta - \beta\gamma)]$$

$$= \frac{1}{m^2}(\alpha\delta - \beta\gamma)(T^2 - dU^2) = \alpha\delta - \beta\gamma,$$

und somit ist die Substitution (22) auch mit der gegebenen gleichartig.

Es kann vorkommen, dass die Coefficienten der Substitution (22) für gewisse Lösungen der unbestimmten Gleichung $t^2 - du^2 = m^2$ gebrochene Zahlen werden. Solche Substitutionen sind natürlich zu verwerfen.

Dieser Fall wird übrigens nie eintreten, wenn die Formen F, F'' äquivalent sind. Dann muss m, als grösster gemeinschaftlicher Divisor von a', $2b'$, c', auch grösster gemeinschaftlicher Divisor von a, $2b$, c sein (§ 99). Nun ist

$$t^2 - du^2 = m^2,$$

also, da $d = b^2 - ac$ ist,

$$t^2 - b^2u^2 = m^2 - ac \,.\, u^2,$$

und da sowohl a, als auch c durch m, die rechte Seite also durch m^2 theilbar ist, so muss auch die linke Seite, und um so mehr $4t^2 - 4b^2u^2$ durch m^2 theilbar sein. $2b$ ist aber durch m, somit $4b^2$ durch m^2 theilbar. Daher wird auch $4t^2$ durch m^2, also $2t$ durch m theilbar sein. Es sind somit

$$\frac{2}{m}(t + bu) \quad \text{und} \quad \frac{2}{m}(t - bu)$$

ganze Zahlen, und da die Differenz beider, d. i. $\frac{4bu}{m}$ gerade ist, so müssen diese Zahlen entweder beide gerade oder beide ungerade sein. Wäre jede derselben ungerade, so würde auch ihr Produkt $\frac{4}{m^2}(t^2 - b^2u^2)$ ungerade sein, was nicht der Fall ist, da m^2 in $t^2 - b^2u^2$ aufgeht. Jene Zahlen sind also gerade, und somit sind

$$\frac{1}{m}(t + bu) \quad \text{und} \quad \frac{1}{m}(t - bu)$$

ganze Zahlen. Da nun sowohl a, als auch c durch m theilbar ist, so erkennen wir, dass die Coefficienten der Substitution (22), die sich auch folgendermassen schreiben lassen:

$$\alpha' = \frac{1}{m}[\alpha(t - bu) - c\gamma u]$$

$$\beta' = \frac{1}{m}[\beta(t - bu) - c\delta u]$$

$$\gamma' = \frac{1}{m}[\gamma(t + bu) + a\alpha u]$$

$$\delta' = \frac{1}{m}[\delta(t + bu) + a\beta u]$$

ganze Zahlen sein werden.

Wenn wir also alle Lösungen der unbestimmten Gleichung

$$t^2 - du^2 = m^2,$$

die uns später beschäftigen wird, ermittelt haben werden, so sind damit alle mit der gegebenen gleichartigen Transformationen von F in F' bestimmt.

Beispiele. I. Die Form $x^2 + 3y^2$ geht durch die Substitution

$$\begin{cases} x = 2x' + 6y' \\ y = 2x' + 4y' \end{cases}$$

in $16x'^2 + 72x'y' + 84y'^2$ über. Hier ist $d = -3$, $m = 4$, also die Gleichung

$$t^2 + 3u^2 = 16$$

zu lösen. Die Wurzeln derselben sind

t	4	−4	2	2	−2	−2
u	0	0	2	−2	2	−2

und diesen entsprechen beziehungsweise die Substitutionen, deren Coefficienten folgende sind:

α	2	−2	−2	4	−4	2
β	6	−6	−3	9	−9	3
γ	2	−2	2	0	0	−2
δ	4	−4	5	−1	1	−5.

II. Die Form $x^2 + 7y^2$ geht durch die Substitution

$$\begin{cases} x = 2x' + 10y' \\ y = 2x' - 6y' \end{cases}$$

über in $32x'^2 - 128x'y' + 352y'^2$. Hier ist $d = -7$, $m = 32$, also die Gleichung

$$t^2 + 7u^2 = 1024$$

zu lösen. Dieselbe hat 10 Lösungen, nämlich

t	31	31	−31	−31	18	18	−18	−18	4	−4
u	3	−3	3	−3	10	−10	10	−10	−12	12

welche Substitutionen mit gebrochenen Coefficienten liefern würden, also zu verwerfen sind. Den übrigen 8 Lösungen

t	32	−32	24	24	−24	−24	4	−4
u	0	0	8	−8	8	−8	12	−12

entsprechen die Substitutionen mit beziehungsweise den Coefficienten

α	$+2$	-2	-2	$+5$	-5	$+2$	-5	$+5$
β	$+10$	-10	$+18$	-3	$+3$	-18	$+17$	-17
γ	$+2$	-2	$+2$	$+1$	-1	-2	$+1$	-1
δ	-6	$+6$	-2	-7	$+7$	$+2$	$+3$	-3.

§ 104. Ambige Formen. — Eine Form (a, b, c) wird ambig genannt, wenn $2b$ durch a theilbar ist. Ambige Formen sind z. B. $(a, 0, c)$, $(2a, a, c)$.

In § 101 haben wir schon bewiesen, dass eine ambige Form sich selbst uneigentlich äquivalent ist. Es muss daher auch jede Form, welche einer ambigen Form äquivalent ist, sich selbst uneigentlich äquivalent sein. Dieser Satz lässt sich aber auch umkehren. Es besteht nämlich der

Lehrsatz. Wenn eine Form sich selbst uneigentlich äquivalent ist, so giebt es stets eine ihr äquivalente ambige Form.

Beweis. Die Form (a, b, c) möge durch die Substitution

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y', \end{cases}$$

deren Determinante $\alpha\delta - \beta\gamma = -1$ ist, in sich selbst transformirt werden, so ist

$$(1) \qquad a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a\,,$$

$$(2) \qquad a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b\,,$$

$$(3) \qquad a\beta^2 + 2b\beta\delta + c\delta^2 = c\,.$$

Nun folgt durch $(1).\delta - (2).\gamma$

$$a\alpha(\alpha\delta - \beta\gamma) + b\gamma(\alpha\delta - \beta\gamma) = a\delta - b\gamma$$

oder, da $\alpha\delta - \beta\gamma = -1$ ist,

$$-a\alpha - b\gamma = a\delta - b\gamma;$$

also ist

$$(4) \qquad a(\alpha + \delta) = 0\,.$$

Weiter folgt durch $(2).(\alpha + \delta) - (1).\beta - (3).\gamma$

$$a\beta(\alpha\delta - \beta\gamma) + b\alpha(\alpha\delta - \beta\gamma) + b\delta(\alpha\delta - \beta\gamma) + c\gamma(\alpha\delta - \beta\gamma)$$
$$= b\alpha + b\delta - a\beta - c\gamma$$

oder

$$-a\beta - ba - b\delta - c\gamma = ba + b\delta - a\beta - c\gamma;$$

also ist

(5) $$b(\alpha + \delta) = 0.$$

Endlich folgt durch (3) . α — (2) . β

$$b\beta(\alpha\delta - \beta\gamma) + c\delta(\alpha\delta - \beta\gamma) = c\alpha - b\beta$$

oder

$$-b\beta - c\delta = c\alpha - b\beta;$$

also ist

(6) $$c(\alpha + \delta) = 0.$$

Aus den Gleichungen (4), (5), (6) geht hervor, dass $\alpha + \delta = 0$, also $\delta = -\alpha$ ist; wäre nämlich $\alpha + \delta$ von Null verschieden, so müsste $a = b = c = 0$ sein, was offenbar unmöglich ist.

Durch (2) . α — (1) . β erhält man noch

$$b\alpha(\alpha\delta - \beta\gamma) + c\gamma(\alpha\delta - \beta\gamma) = b\alpha - a\beta$$

oder

$$-b\alpha - c\gamma = b\alpha - a\beta;$$

es ist also

(7) $$a\beta - 2b\alpha - c\gamma = 0,$$

und diese Formel wird uns unten von Nutzen sein.

Wird in der Gleichung $\alpha\delta - \beta\gamma = -1$ die Grösse δ durch den dafür erhaltenen Werth $-\alpha$ ersetzt, so erhält man

$$\alpha^2 - 1 = -\beta\gamma \quad \text{oder} \quad \frac{\alpha + 1}{\gamma} = \frac{\beta}{1 - \alpha}.$$

In den kleinsten Zahlen, die möglich sind, ausgedrückt, sei dieses Verhältniss $= \frac{m}{n}$; dann sind also m und n prim zu einander. Ferner seien zwei ganze Zahlen μ, ν so bestimmt, dass

$$m\mu + n\nu = 1$$

ist. Dann behaupten wir,

(8) $$\begin{cases} x = mx'' - \nu y'' \\ y = nx'' + \mu y'' \end{cases}$$

sei eine Substitution, welche F in eine äquivalente ambige Form G transformire. Da die Determinante der Substitution (8) den Werth $+1$ hat, so ist G eigentlich äquivalent F. Wir haben also nur zu beweisen, dass G eine ambige Form ist. Zu diesem Zwecke berechnen wir die beiden ersten Coefficienten der Form $G = (a', b', c')$. Es ergiebt sich

$$(9)\qquad \begin{cases} a' = am^2 + 2bmn + cn^2, \\ 2b' = -2am\nu - 2bn\nu + 2bm\mu + 2cn\mu. \end{cases}$$

Nun folgt aus der Relation $\frac{\beta}{1-\alpha} = \frac{m}{n}$, dass

$$\beta n + \alpha m - m = 0$$

ist, und aus $\frac{\alpha + 1}{\gamma} = \frac{m}{n}$, dass

$$\gamma m - \alpha n - n = 0$$

ist. Es hat also jede der drei Zahlen

$$g = 1 - m\mu - n\nu,$$
$$h = \beta n + \alpha m - m,$$
$$k = \gamma m - \alpha n - n$$

den Werth Null, und der Ausdruck

$$m^2(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2)$$

bleibt unverändert, wenn man

$$g[(m\mu + 1)\beta - (\alpha + 1)m\nu] + h(m\mu\nu + \nu) + km\nu^2$$

dazu zählt. Durch Ausführung der Rechnung erhält man nach leichten Reductionen

$$m^2(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2) = -2m\nu + \beta.$$

Ebenso bleibt

$$mn(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2)$$

unverändert, wenn man

$$g[(m\mu - n\nu) - (1 + \mu m + n\nu)\alpha] - hm\mu^2 + kn\nu^2$$

dazu zählt, und man erhält

$$mn(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2) = m\mu - n\nu - \alpha.$$

Endlich erleidet auch

$$n^2(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2)$$

durch Addition von

$$-g[n\mu(\alpha - 1) + (n\nu + 1)\gamma] - hn\mu^2 - k(n\mu\nu + \mu)$$

keine Veränderung, und es ergiebt sich

$$n^2(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2) = 2n\mu - \gamma.$$

Es ist also

$$(am^2 + 2bmn + cn^2)(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2)$$
$$= -2am\nu + a\beta + 2bm\mu - 2bn\nu - 2b\alpha + 2cn\mu - c\gamma$$
$$= (-2am\nu + 2bm\mu - 2bn\nu + 2cn\mu) + (a\beta - 2b\alpha - c\gamma)$$

oder wegen (9) und (7)

$$a'(\beta\mu^2 - 2\alpha\mu\nu - \gamma\nu^2) = 2b';$$

a' geht also in $2b'$ auf, und somit ist G eine ambige Form.

Beispiel. Die Form (3, 13, 18) geht durch die Substitution

$$\begin{cases} x = 3x' + 2y' \\ y = -4x' - 3y', \end{cases}$$

deren Determinante -1 ist, in sich selbst über, ist also sich selbst uneigentlich äquivalent. Hier ist

$$\frac{\alpha + 1}{\gamma} = \frac{4}{-4} = \frac{m}{n} = -1.$$

Man kann also erstens $m = 1$, $n = -1$ annehmen; dann hat man die Gleichung

$$\mu - \nu = 1$$

zu lösen. Der Lösung $\mu = 1$, $\nu = 0$ entspricht die Substitution $x = x'$, $y = -x' + y'$, durch welche (3, 13, 18) in $(-5, -5, 18)$ übergeht. Der Lösung $\mu = 2$, $\nu = 1$ entspricht die Substitution $x = x' - y'$, $y = -x' + 2y'$, welche (3, 13, 18) in $(-5, 0, 23)$ transformirt, u. s. w.

Wird zweitens $m = -1$, $n = 1$ angenommen, so ist die Hülfsgleichung $-\mu + \nu = 1$.

Der Lösung $\mu = 0$, $\nu = 1$ dieser Gleichung entspricht die Substitution $x = -x' - y'$, $y = x'$, welche (3, 13, 18) in $(-5, -10, 3)$ verwandelt. Der Lösung $\mu = 1$, $\nu = 2$ entspricht die Substitution

$$x = -x' - 2y', \qquad y = x' + y',$$

welche die ambige Form $(-5, -15, -22)$ liefert, u. s. w.

Aufgabe 1. Die Form $(7, 1, -1)$ geht durch die Substitution $x = 2x' + y'$, $y = -3x' - 2y'$, deren Determinante -1 ist, in sich selbst über, ist also sich selbst uneigentlich äquivalent. Man soll einige jener Form äquivalente ambige Formen bilden.

[(4, 2, − 1), (4, − 2, − 1), (4, − 6, 7), ...].

Aufgabe 2. Man hat eine ambige Form G durch eine Substitution

$$\begin{cases} \xi = \alpha x + \beta y \\ \eta = \gamma x + \delta y, \end{cases}$$

deren Determinante $+1$ ist, in eine Form F transformirt. Es soll nun eine Transformation mit der Determinante -1 ermittelt werden, welche F in sich selbst transformire.

Lösung. Nach § 98 wird F in G transformirt durch die Substitution

$$(1) \qquad \begin{cases} x = \delta x' - \beta y' \\ y = -\gamma x' + \alpha y'; \end{cases}$$

weiter wird G in sich selbst transformirt durch die Substitution

$$(2) \qquad \begin{cases} x' = x'' + k y'' \\ y' = \qquad -y'', \end{cases}$$

wo k die ganze Zahl $\frac{2b}{a}$ bezeichnet; endlich geht G in F über, wenn man

$$(3) \qquad \begin{cases} x'' = \alpha x''' + \beta y''' \\ y'' = \gamma x''' + \delta y''' \end{cases}$$

setzt; F wird also in sich selbst transformirt, wenn man die Substitutionen (1), (2), (3), deren Determinanten beziehungsweise $+1$, -1, $+1$ sind, nach einander anwendet, oder durch die Substitution

$$(4) \qquad \begin{cases} x = (\alpha\delta + \beta\gamma + k\gamma\delta)\, x''' + (2\beta\delta + k\delta^2) y''' \\ y = -(2\alpha\gamma + k\gamma^2) \quad x''' - (\alpha\delta + \beta\gamma + k\gamma\delta) y''', \end{cases}$$

und die Determinante dieser letzteren ist -1.

Beispiel. (2, 1, 7) verwandelt sich in (34, -15, 7) durch die Substitution

$$\xi = 3x - y, \quad \eta = -2x + y,$$

also wird (34, -15, 7) in (2, 1, 7) transformirt durch die Substitution

$$x = x' + y', \quad y = 2x' + 3y';$$

(2, 1, 7) bleibt unverändert, wenn man

$$x' = x'' + y'', \quad y' = -y''$$

setzt; endlich geht (2, 1, 7) in (34, -15, 7) über durch die Substitution

$$x'' = 3x''' - y''', \quad y'' = -2x''' + y''';$$

somit transformirt sich (34, — 15, 7) in sich selbst, wenn

$$\begin{cases} x = x' + y' \\ y = 2x' + 3y', \end{cases} \quad \begin{cases} x' = x'' + y'' \\ y' = \quad - y'', \end{cases} \quad \begin{cases} x'' = 3x''' - y''' \\ y'' = -2x''' + y''', \end{cases}$$

oder direkt

$$\begin{cases} x = 3x''' - \ y''' \\ y = 8x''' - 3y''' \end{cases}$$

gesetzt wird.

§ 105. Beziehung der Darstellungen einer Zahl M durch eine Form (a, b, c) zu den Wurzeln der Congruenz $\xi^2 \equiv b^2 - ac \pmod{M}$. — Wenn den unbestimmten Grössen x, y bestimmte Werthe m, n beigelegt werden, so nimmt die Form (a, b, c) einen bestimmten Werth M an. Man sagt dann, die Zahl M werde durch die Form (a, b, c) dargestellt, und zwar heisst die Darstellung eine eigentliche oder eine uneigentliche, je nachdem die Werthe m, n, die man für x, y setzt, prim zu einander sind oder nicht. Die Darstellungen einer Zahl M durch eine Form (a, b, c) stehen in einem interessanten Zusammenhange mit den Wurzeln der Congruenz $\xi^2 \equiv D \pmod{M}$, wo $D = b^2 - ac$ die Determinante der Form (a, b, c) ist, und dieser Zusammenhang wird durch die folgenden Sätze ausgedrückt:

Lehrsatz I. Die Determinante D einer Form (a, b, c), durch welche eine eigentliche Darstellung einer Zahl M möglich ist, ist ein quadratischer Rest von M.

Beweis. Es seien m, n die Werthe, die man beziehungsweise x, y beilegen muss, damit die Form (a, b, c) gleich M werde, also

$$am^2 + 2bmn + cn^2 = M.$$

Da nun m prim zu n ist, so lassen sich zwei ganze Zahlen μ, ν bestimmen, welche der Bedingung

$$\mu m + \nu n = 1$$

genügen. Dann geht die leicht zu bestätigende Identität

$$(am^2 + 2bmn + cn^2)(a\nu^2 - 2b\mu\nu + c\mu^2)$$
$$= [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac)(\mu m + \nu n)^2$$

über in

$$M(a\nu^2 - 2b\mu\nu + c\mu^2)$$
$$= [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac).$$

Es ist also

$$[\mu(mb + nc) - \nu(ma + nb)]^2 \equiv b^2 - ac \pmod{M},$$

d. h. $b^2 - ac$ ist in der That quadratischer Rest von M.

Dieser Satz liefert zugleich einen Ausdruck für die Wurzeln der Congruenz $\xi^2 \equiv b^2 - ac \pmod{M}$, nämlich

$$\mu(mb + nc) - \nu(ma + nb).$$

Nun hat aber die Gleichung

$$\mu m + \nu n = 1$$

unendlich viele Lösungen μ, ν, und jeder dieser Lösungen entspricht ein Werth jenes Ausdrucks. In welcher Beziehung diese letzteren zu einander stehen, sagt uns der folgende Satz:

Lehrsatz II. Eine jede eigentliche Darstellung $x = m$, $y = n$ einer Zahl M durch eine Form (a, b, c) liefert, welche Werthe man auch für μ, ν wählen mag, nur eine einzige Wurzel der Congruenz

$$\xi^2 \equiv b^2 - ac \pmod{M}.$$

Beweis. Es sei $\mu m + \nu n = 1$ und zugleich

$$\mu' m + \nu' n = 1,$$

so erhält man durch Elimination von m

$$n(\mu'\nu - \mu\nu') = \mu' - \mu$$

und durch Elimination von n

$$m(\mu\nu' - \mu'\nu) = \nu' - \nu.$$

Wenn man nun die den Werthepaaren μ, ν und μ', ν' entsprechenden Werthe des Ausdrucks, welcher die Wurzeln der Congruenz $\xi^2 \equiv b^2 - ac \pmod{M}$ darstellt, beziehungsweise mit v, v' bezeichnet, also

$$v = \mu(mb + nc) - \nu(ma + nb),$$
$$v' = \mu'(mb + nc) - \nu'(ma + nb)$$

setzt, so erhält man durch Subtraction

$$v' - v = (\mu' - \mu)(mb + nc) - (\nu' - \nu)(ma + nb)$$

oder bei Anwendung der oben für $\mu' - \mu$ und $\nu' - \nu$ gefundenen Werthe

$$v' - v = n(\mu'\nu - \mu\nu')(mb + nc) - m(\mu\nu' - \mu'\nu)(ma + nb)$$
$$= (\mu'\nu - \mu\nu')(am^2 + 2bmn + cn^2)$$
$$= (\mu'\nu - \mu\nu')\, M.$$

Es ist also wirklich

$$v \equiv v' \pmod{M}.$$

Beispiel. Die Form $(7, -2, 3)$, deren Determinante -17 ist, nimmt den Werth 31 an, wenn man $x = 2$, $y = 3$ setzt, und die Gleichung

$$2\mu + 3\nu = 1$$

hat die Lösungen

μ	-1	$+2$	$+5$	$+8$	$\dots$
ν	1	-1	-3	-5	$\dots$

Da nun hier

$$mb + nc = -4 + 9 = 5,$$
$$ma + nb = 14 - 6 = 8$$

ist, so erhält man

$$v = -13, \quad v' = +18, \quad v'' = +49, \quad v''' = +80, \dots$$

Alle diese Zahlen genügen der Congruenz

$$\xi^2 \equiv -17 \pmod{31},$$

aber da sie mod. 31 congruent sind, so haben wir sie als eine einzige Wurzel dieser Congruenz anzusehen.

Aufgabe. Es sei v_1 der Werth, welchen der Ausdruck

$$(1) \qquad \mu(mb + nc) - \nu(ma + nb)$$

für eine bestimmte Lösung μ_1, ν_1 der Gleichung

$$\mu m + \nu n = 1$$

annimmt, und v_2 eine Zahl, welche $\equiv v_1 \pmod{M}$ ist. Man soll die Werthe μ_2, ν_2 von μ, ν ermitteln, für welche der Ausdruck (1) gleich v_2 wird.

Lösung. Zur Bestimmung von μ_2, ν_2 hat man die beiden Gleichungen

$$m\mu_2 + n\nu_2 = 1,$$
$$\mu_2(mb + nc) - \nu_2(ma + nb) = v_2,$$

aus denen durch Elimination von ν_2

$$\mu_2[m(ma + nb) + n(mb + nc)] = ma + nb + nv_2$$

oder kürzer

$$\mu_2 M = ma + nb + nv_2,$$

und durch Elimination von μ_2

$$v_2[m(ma + nb) + n(mb + nc)] = mb + nc - mv_2$$

oder kürzer $v_2 M = mb + nc - mv_2$ folgt.

Es ist also

$$\mu_2 M = ma + nb + nv_2$$

und ebenso natürlich

$$\mu_1 M = ma + nb + nv_1,$$

also

$$M(\mu_2 - \mu_1) = n(v_2 - v_1)$$

oder

$$\mu_2 = \mu_1 + \frac{n(v_2 - v_1)}{M}.$$

Auf dieselbe Weise erhält man durch Subtraction der beiden Gleichungen

$$v_2 M = mb + nc - mv_2,$$
$$v_1 M = mb + nc - mv_1$$

für v_2 den Werth

$$v_2 = v_1 - \frac{m(v_2 - v_1)}{M}.$$

Beispiel. Wir nehmen wieder die oben betrachtete Form $(7, -2, 3)$ und die Darstellung $x = 2$, $y = 3$ der Zahl 31 durch dieselbe. Für die Lösung $\mu_1 = 5$, $v_1 = -3$ der Gleichung $2\mu + 3v = 1$ liefert der Ausdruck (1), da

$$mb + nc = 5, \quad ma + nb = 8$$

ist, die Wurzel $v_1 = 49$ der Congruenz

$$x^2 \equiv -17 \pmod{31}.$$

Um die Werthe μ_2, v_2 zu erhalten, welche die Wurzel 235 derselben Congruenz liefern würden, haben wir nur

$$\mu_2 = \quad 5 + \frac{3 \cdot (235 - 49)}{31} = \quad 23,$$

$$v_2 = -3 - \frac{2 \cdot (235 - 49)}{31} = -15$$

anzunehmen.

Eine jede eigentliche Darstellung $x = m$, $y = n$ der Zahl M durch die Form (a, b, c) entspricht also einer bestimmten

Wurzel v der Congruenz $\xi^2 \equiv b^2 - ac \pmod{M}$ oder, wie wir dafür zuweilen auch sagen werden, einem bestimmten Werthe v des Ausdrucks $\sqrt{b^2 - ac} \pmod{M}$. Man sagt dann: diese Darstellung gehört zum Werthe v des Ausdrucks $\sqrt{b^2 - ac} \pmod{M}$.

Hat man zwei eigentliche Darstellungen einer Zahl M durch eine Form (a, b, c), nämlich $x = m$, $y = n$ und $x = m'$, $y = n'$, ist also

$$M = am^2 + 2bmn + cn^2,$$
$$M = am'^2 + 2bm'n' + cn'^2$$

und zugleich

$$\mu m + \nu n = 1,$$
$$\mu' m' + \nu' n' = 1,$$

so liefert die erste Darstellung die Wurzel

$$v = \mu(mb + nc) - \nu(ma + nb),$$

die zweite die Wurzel

$$v' = \mu'(m'b + n'c) - \nu'(m'a + n'b)$$

der Congruenz $\xi^2 \equiv b^2 - ac \pmod{M}$, und es sind drei Fälle zu unterscheiden:

Erstens kann für irgend ein Werthepaar μ, ν und irgend ein Werthepaar μ', ν'

$$v \equiv v' \pmod{M}$$

sein. In diesem Falle besteht die Congruenz [da die Anwendung anderer passender Werthe von μ, ν, resp. μ', ν' doch zu denselben, d. h. mod. M congruenten Werthen von v, resp. v' führt] für alle Werthe, die man μ, ν, resp. μ', ν' beilegen kann; beide Darstellungen gehören also zu demselben Werthe des Ausdrucks $\sqrt{b^2 - ac} \pmod{M}$.

Wenn zweitens die Congruenz $v \equiv v' \pmod{M}$ für irgend ein Werthepaar μ, ν und irgend ein Werthepaar μ', ν' nicht besteht, so kann sie überhaupt für keine Werthe stattfinden, die μ, ν, resp. μ', ν' beigelegt werden können; in diesem Falle gehören die beiden Darstellungen zu verschiedenen Werthen von $\sqrt{b^2 - ac} \pmod{M}$.

Wenn drittens $v \equiv -v' \pmod{M}$ ist, so gehören

beide Darstellungen zu entgegengesetzten Werthen von $\sqrt{b^2 - ac}$ (mod. M).

Beispiel. Die Form (4, 6, — 14), deren Determinante = 92 ist, nimmt den Werth 1106 an, wenn man

$$1.\ x = 20,\quad y = 19$$
$$2.\ x = 28,\quad y = 29$$
$$3.\ x = 13,\quad y = 5$$
$$4.\ x = -28,\quad y = 5$$

setzt. Nun hat die Gleichung

$20\mu + 19\nu = 1$ die Wurzeln $\mu = 1,\ \nu = -1$
$28\mu + 29\nu = 1$ „ „ $\mu = -1,\ \nu = 1$
$13\mu + 5\nu = 1$ „ „ $\mu = 2,\ \nu = -5$
$-28\mu + 5\nu = 1$ „ „ $\mu = -2,\ \nu = -11$.

Es gehören also unsere 4 Darstellungen von 1106 durch die Form (4, 6, — 14) beziehungsweise zu den Wurzeln

$$v_1 = (20.6 - 19.14) + (20.4 + 19.6) = +48$$
$$v_2 = -(28.6 - 29.14) - (28.4 + 29.6) = -48$$
$$v_3 = 2(13.6 - 5.14) + 5(13.4 + 5.6) = +426$$
$$v_4 = -2(-28.6 - 5.14) + 11(-28.4 + 5.6) = -426$$

der Congruenz $\xi^2 \equiv 92$ (mod. 1106). Die erste und die dritte Darstellung gehören also zu verschiedenen, die erste und die zweite, wie auch die dritte und die vierte zu entgegengesetzten Werthen des Ausdrucks $\sqrt{92}$ (mod. 1106).

§ 106. Darstellungen einer Zahl durch äquivalente Formen. —

Lehrsatz I. Eine Zahl M lässt sich durch eine Form F mindestens ebenso oft darstellen, wie durch eine unter F enthaltene Form F'.

Beweis. Wenn die Form F durch die Substitution

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases}$$

in F' übergeht und F' für $x' = m$, $y' = n$ gleich M wird, so nimmt offenbar auch F den Werth M an, wenn man

$$x = \alpha m + \beta n,\quad y = \gamma m + \delta n$$

setzt.

Ebenso wird, wenn $x' = m'$, $y' = n'$ eine zweite, von der ersten verschiedene Darstellung von M durch F' ist, auch

$$x = \alpha m' + \beta n', \; y = \gamma m' + \delta n'$$

eine zweite Darstellung von M durch F sein, und wir haben nur zu zeigen, dass diese letztere von der ersteren (d. i. $x = \alpha m + \beta n$, $y = \gamma m + \delta n$) verschieden ist.

Wäre gleichzeitig

$$\alpha m + \beta n = \alpha m' + \beta n',$$
$$\gamma m + \delta n = \gamma m' + \delta n',$$

so würde man durch Elimination von n

$$m\,(\alpha\delta - \beta\gamma) = m'\,(\alpha\delta - \beta\gamma)$$

und durch Elimination von m

$$n\,(\alpha\delta - \beta\gamma) = n'\,(\alpha\delta - \beta\gamma)$$

erhalten; es würden also die beiden Gleichungen

$$(\alpha\delta - \beta\gamma)\,(m - m') = 0,$$
$$(\alpha\delta - \beta\gamma)\,(n - n') = 0$$

bestehen, und da der Voraussetzung nach nicht gleichzeitig $m = m'$, $n = n'$ sein soll, so müsste $\alpha\delta - \beta\gamma$, also auch die Determinante von F' gleich Null sein. Solche Formen haben wir aber vorläufig ausdrücklich von der Betrachtung ausgeschlossen. Die Darstellungen der Zahl M durch die Form F, welche den verschiedenen Darstellungen von M durch F' entsprechen, sind daher sämmtlich von einander verschieden, und somit lässt sich M durch F mindestens ebenso oft darstellen wie durch F'.

Zusatz I. Eine Zahl M lässt sich durch die eine von zwei äquivalenten Formen genau so oft darstellen wie durch die andere.

Zuzatz II. Sind F, F' zwei äquivalente Formen und

$$\begin{cases} x' = m \\ y' = n \end{cases} \quad \text{und} \quad \begin{cases} x = \alpha m + \beta n \\ y = \gamma m + \delta n \end{cases}$$

zwei einander entsprechende Darstellungen der Zahl M durch beziehungsweise F' und F, so ist der grösste gemeinschaftliche Divisor von m und n gleich dem

grössten gemeinschaftlichen Divisor von $\alpha m + \beta n$ und $\gamma m + \delta n$.

Beweis. Ist d der grösste gemeinschaftliche Divisor von m und n, so kann man nach § 24, VI zwei ganze Zahlen μ, ν bestimmen, welche der Gleichung

$$\mu m + \nu n = d$$

genügen. Nun besteht die Identität

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n)$$
$$= (\alpha\delta - \beta\gamma)(\mu m + \nu n),$$

und diese geht, da

$$\alpha\delta - \beta\gamma = \pm 1, \; \mu m + \nu n = d$$

ist, über in

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = \pm d,$$

woraus hervorgeht, dass der grösste gemeinschaftliche Divisor von $\alpha m + \beta n$ und $\gamma m + \delta n$ auch in d aufgehen wird. Da nun aber d als grösster gemeinschaftlicher Divisor von m und n sowohl in $\alpha m + \beta n$, als auch in $\gamma m + \delta n$ aufgeht, so wird d selbst der grösste gemeinschaftliche Divisor von $\alpha m + \beta n$ und $\gamma m + \delta n$ sein.

Wenn im Besonderen m prim zu n ist, so ist auch $\alpha m + \beta n$ prim zu $\gamma m + \delta n$.

Lehrsatz II. Es seien

$$F = ax^2 + 2bxy + cy^2,$$
$$F' = a'x'^2 + 2b'x'y' + c'y'^2$$

zwei äquivalente Formen der Determinante D, und es möge F' in F durch die Substitution

$$\begin{cases} x' = \alpha x + \beta y \\ y' = \gamma x + \delta y, \end{cases}$$

deren Determinante $\alpha\delta - \beta\gamma = \varepsilon = \pm 1$ sei, übergehen. Ist dann $x = m$, $y = n$ eine eigentliche Darstellung einer Zahl M durch die Form F, somit

$$x' = \alpha m + \beta n = m', \; y' = \gamma m + \delta n = n'$$

eine eigentliche Darstellung von M durch F', so gehören beide Darstellungen zu demselben Werthe von $\sqrt{D}$ (mod. M) oder zu entgegengesetzten Werthen dieses

Ausdrucks, je nachdem die Transformation von F' in F eine eigentliche oder eine uneigentliche, d. h. je nachdem $\varepsilon = +1$ oder $= -1$ ist.

Beweis. Da der grösste gemeinschaftliche Divisor von m, n die Einheit ist, so lassen sich zwei ganze Zahlen μ, ν so bestimmen, dass man

$$\mu m + \nu n = 1$$

hat, und die Identität des letzten Zusatzes geht über in

$$\varepsilon(\delta\mu - \gamma\nu)\, m' - \varepsilon(\beta\mu - \alpha\nu)\, n' = +1$$

oder, wenn

$$\varepsilon(\delta\mu - \gamma\nu) = \mu', \quad -\varepsilon(\beta\mu - \alpha\nu) = \nu'$$

gesetzt wird, in

$$\mu' m' + \nu' n' = 1.$$

Nun gehört nach § 105 die Darstellung $x = m$, $y = n$ zum Werthe

$$v = \mu(mb + nc) - \nu(ma + nb)$$

des Ausdrucks $\sqrt{D}$ (mod. M), und durch Einsetzung der in § 98 (4) gegebenen Werthe von a, b, c erhält man hieraus

$$\begin{aligned} v = \mu\, \{ & m\,[a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta] \\ & + n\,[a'\beta^2 + 2b'\beta\delta + c'\delta^2]\} \\ - \nu\, \{ & m\,[a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2] \\ & + n\,[a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta]\}. \end{aligned}$$

Ebenso gehört die Darstellung $x' = m'$, $y' = n'$ zu dem Werthe

$$v' = \mu'(m'b' + n'c') - \nu'(m'a' + n'b'),$$

und durch Einsetzung der für μ', ν', m', n' gegebenen Werthe verwandelt sich dieser Ausdruck in εv. Es ist also

$$v' = \varepsilon v,$$

d. h. $v' = +v$ oder $= -v$, je nachdem eigentliche oder uneigentliche Aequivalenz stattfindet.

Wenn es also mehrere zu verschiedenen Werthen von $\sqrt{D}$ (mod. M) gehörende eigentliche Darstellungen von M durch die Form (a, b, c) giebt, so werden die entsprechenden Darstellungen durch die äquivalente Form (a', b', c') zu denselben Werthen von $\sqrt{D}$ (mod. M) gehören, und wenn es für einen bestimmten Werth von $\sqrt{D}$ (mod. M) keine eigentliche Dar-

stellung von M durch eine Form giebt, so wird auch keine dieser äquivalente Form eine zu diesem Werthe gehörende Darstellung liefern.

Lehrsatz III. Ist $x = m$, $y = n$ eine eigentliche Darstellung der (von Null verschiedenen) Zahl M durch die Form (a, b, c) und v der Werth von

$$\sqrt{D} = \sqrt{b^2 - ac} \pmod{M},$$

zu welchem diese Darstellung gehört, so sind die beiden Formen (a, b, c) und $\left(M, v, \frac{v^2 - D}{M}\right)$ eigentlich äquivalent.

Beweis. Wenn wir wieder zwei ganze Zahlen μ, ν bestimmen, welche der Gleichung

$$\mu m + \nu n = 1$$

genügen, so ist

$$v = \mu (bm + cn) - \nu (am + bn).$$

Nun verwandelt sich die Form (a, b, c) durch die Substitution

$$\begin{cases} x = mx' - \nu y' \\ y = nx' + \mu y', \end{cases}$$

da $m\mu + n\nu = +1$ ist, in eine eigentlich äquivalente Form (a', b', c'), und es ist nach § 98 (4)

$$\begin{aligned} a' &= am^2 + 2bmn + cn^2 = M, \\ b' &= -am\nu + b(m\mu - n\nu) + cn\mu \\ &= \mu (bm + cn) - \nu (am + bn) = v; \end{aligned}$$

es soll aber auch $b'^2 - a'c' = D$, also $v^2 - Mc' = D$ sein, und daraus folgt

$$c' = \frac{v^2 - D}{M}.$$

Die äquivalente Form, in welche (a, b, c) durch jene Substitution transformirt wird, ist also

$$\left(M, v, \frac{v^2 - D}{M}\right).$$

Für die Zahlen μ, ν erhält man übrigens durch Auflösung der beiden Gleichungen

$$\mu m + \nu n = 1, \quad \mu (bm + cn) - \nu (am + bn) = v$$

die Werthe

$$\mu = \frac{am + bn + vn}{M}, \quad \nu = \frac{bm + cn - vm}{M},$$

und somit ist auch die Substitution vollständig bekannt.

Ist $x = m'$, $y = n'$ eine zweite, zu demselben Werthe v von $\sqrt{D}$ (mod. M) gehörende eigentliche Darstellung der Zahl M durch die Form (a, b, c), so liefert die Substitution

$$\begin{cases} x = m'x' - \nu'y' \\ y = n'x' + \mu'y' \end{cases},$$

wo

$$\mu' = \frac{am' + bn' + vn'}{M}, \quad \nu' = \frac{bm' + cn' - vm'}{M}$$

ist, eine zweite (a, b, c) äquivalente Form.

Umgekehrt folgt aus jeder eigentlichen Transformation von F in eine äquivalente Form eine zu einem bestimmten Werthe v von $\sqrt{D}$ (mod. M) gehörende Darstellung der Zahl M durch die Form F. Geht nämlich (a, b, c) durch die Substitution

$$\begin{cases} x = mx' - \nu y' \\ y = nx' + \mu y' \end{cases},$$

deren Determinante $+1$ ist, in die äquivalente Form F' über, so ist $x = m$, $y = n$ eine eigentliche Darstellung von M durch F, und der Werth von $\sqrt{D}$ (mod. M), zu welchem dieselbe gehört, ist

$$v = \mu(mb + nc) - \nu(ma + nb).$$

Wenn man also alle eigentlichen Transformationen von F in eine äquivalente Form $\left(M, v, \frac{v^2 - D}{M}\right)$ hat, so ergeben sich daraus alle zu dem Werthe v von $\sqrt{D}$ (mod. M) gehörenden Darstellungen der Zahl M durch die Form F, und somit ist die Ermittlung aller eigentlichen Darstellungen von M durch F darauf zurückgeführt, alle eigentlichen Transformationen von F in eine gegebene äquivalente Form zu bestimmen. Da wir nun in § 103 gelernt haben, wie man aus einer gegebenen Transformation alle mit derselben gleichartigen Transformationen herleitet, so sind wir im Stande, aus einer Darstellung von M durch F alle zu demselben Werthe v gehörenden Darstellungen zu bilden.

Ist nämlich $x = x_1$, $y = y_1$ eine zum Werthe v des

Ausdrucks $\sqrt{D}$ (mod. M) gehörende Darstellung der Zahl M durch die Form (a, b, c), deren Determinante D ist, und bezeichnet m den grössten gemeinschaftlichen Divisor der Zahlen a, $2b$, c, so werden alle zu demselben Werthe v gehörenden Darstellungen durch die Formeln

$$x = \frac{x_1 t - (x_1 b + y_1 c) u}{m},$$

$$y = \frac{y_1 t + (x_1 a + y_1 b) u}{m}$$

ausgedrückt, wo für t, u alle Lösungen der unbestimmten Gleichung $t^2 - Du^2 = m^2$ zu setzen sind.

Wenn G eine F äquivalente ambige Form ist, so ist G auch der Form $\left(M, v, \frac{v^2 - D}{M}\right)$ äquivalent; somit sind die Formen F und $\left(M, v, \frac{v^2 - D}{M}\right)$ sowohl eigentlich, als auch uneigentlich äquivalent, oder F ist sowohl $\left(M, v, \frac{v^2 - D}{M}\right)$, als auch $\left(M, -v, \frac{v^2 - D}{M}\right)$ eigentlich äquivalent; wir werden somit sowohl die zum Werthe v, als auch die zum Werthe $-v$ gehörenden Darstellungen der Zahl M durch die Form F erhalten.

Wenn man umgekehrt mehrere Darstellungen der Zahl M durch die Form F hat, welche zu entgegengesetzten Werthen v, $-v$ des Ausdrucks $\sqrt{D}$ (mod. M) gehören, so wird die Form F der Form $\left(M, v, \frac{v^2 - D}{M}\right)$ sowohl eigentlich, als auch uneigentlich äquivalent sein; es wird sich also eine F äquivalente ambige Form G angeben lassen.

Die Aufgabe, deren Lösung uns obliegt, ist die Ermittlung aller Darstellungen einer gegebenen Zahl durch eine gegebene Form. Wie sich die uneigentlichen Darstellungen aus den eigentlichen ergeben, werden wir weiter unten sehen. Vorläufig handelt es sich nur um eigentliche Darstellungen, und wir wollen uns nochmals vergegenwärtigen, wie weit uns unsere bisherigen Betrachtungen geführt haben:

Es sei also eine Zahl M und eine Form $F = (a, b, c)$, deren Determinante D ist, gegeben. Um zu sehen, ob M

durch F dargestellt werden kann, haben wir zunächst die Congruenz $\xi^2 \equiv D \pmod{M}$ zu betrachten. Ist dieselbe unmöglich (d. h. D ein quadratischer Nichtrest von M), so giebt es keine Darstellung von M durch F. Ist dagegen v eine der Wurzeln dieser Congruenz, so haben wir die neue Form $\left(M, v, \frac{v^2-D}{M}\right)$ zu bilden und zu untersuchen, ob dieselbe F eigentlich äquivalent ist oder nicht. Findet keine Aequivalenz statt, so gehört zu v keine Darstellung. Sind aber beide Formen äquivalent, so haben wir eine eigentliche Transformation

$$x = mx' - \nu y', \; y = nx' + \mu y'$$

von F in $\left(M, v, \frac{v^2-D}{M}\right)$ zu suchen, und es ist dann $x = m$, $y = n$ eine erste zur Wurzel v gehörende Darstellung von M durch F. Die übrigen Darstellungen, die zu dieser Wurzel gehören, werden darauf durch die oben gegebenen Formeln geliefert.

Werden in dieser Weise der Reihe nach alle Wurzeln v der Congruenz $\xi^2 \equiv D \pmod{M}$ behandelt, so erhalten wir nach und nach alle Darstellungen von M durch F.

Da die Auflösung der rein quadratischen Congruenz $\xi^2 \equiv D \pmod{M}$ im vorigen Kapitel ihre Erledigung gefunden hat, so ist die Bestimmung aller eigentlichen Darstellungen einer gegebenen Zahl durch eine gegebene Form auf die Lösung der beiden folgenden Aufgaben zurückgeführt:

1. zu untersuchen, ob zwei gegebene Formen F, F' einer Determinante $D = b^2 - ac$ eigentlich äquivalent seien oder nicht, und im ersteren Falle eine eigentliche Transformation der einen in die andere zu finden;

2. die Gleichung $t^2 - Du^2 = m^2$, in welcher m der grösste gemeinschaftliche Divisor der Zahlen a, $2b$, c ist, in ganzen Zahlen aufzulösen und mittels dieser Lösungen alle Transformationen von F in F' zu bilden, welche mit der einen schon gefundenen Transformation gleichartig sind.

Die Behandlung dieser beiden Aufgaben ist eine ganz verschiedene, je nachdem die Determinante D der gegebenen Form eine positive oder eine negative Zahl ist. Wir werden im folgenden Kapitel den Gegenstand zunächst für negative Determinanten behandeln.

Neuntes Kapitel.

Quadratische Formen mit negativer Determinante.

§ 107. Reducirte Formen. — Bei einer Form (a, b, c), deren Determinante $b^2 - ac$ eine negative Zahl ist, hat der erste Coefficient nothwendig dasselbe Zeichen wie der dritte. Wir wollen nun, wie schon früher, den absoluten Werth einer Zahl dadurch ausdrücken, dass wir die Zahl in eine eckige Klammer [] setzen. Wenn dann

$$[c] \geqq [a] > [2b]$$

ist, so nennt man die Form eine reducirte. Von dieser Art sind z. B. die Formen

$$(\pm 5, 2, \pm 6), (\pm 5, -2, \pm 6), (\pm 3, 1, \pm 3),$$
$$(\pm 3, -1, \pm 3), (\pm 4, 2, \pm 5), (\pm 4, -2, \pm 5).$$

Lehrsatz. Für jede Form von negativer Determinante lässt sich eine derselben eigentlich äquivalente reducirte Form ermitteln.

Beweis. Wenn die Form (a, b, a_1), deren Determinante $-D$ ist (D bezeichnet also eine positive Zahl), nicht den Bedingungen einer reducirten Form entspricht, so nehmen wir den absolut kleinsten Rest von $-b$ in Beziehung auf den Modul a_1; dieser Rest sei b_1. Dann ist $b_1 \equiv -b$, also $b_1^2 \equiv b^2$ und $b_1^2 + D \equiv b^2 + D$ (mod. a_1). Die Zahl $b^2 + D$ hat aber den Werth aa_1; somit ist $b_1^2 + D \equiv aa_1 \equiv 0$ (mod. a_1), oder es ist $\frac{b_1^2 + D}{a_1}$ eine ganze Zahl, die wir a_2 nennen wollen. Bilden wir jetzt die neue Form (a_1, b_1, a_2), so ist dieselbe, weil $b + b_1 \equiv 0$ (mod. a_1) ist, der gegebenen Form (a, b, a_1) nach rechts benachbart, also sind beide Formen eigentlich äquivalent. Da ferner der absolut kleinste Rest einer Zahl

für irgend einen Modul höchstens gleich der Hälfte dieses Moduls, also $[b_1] \leq [\frac{1}{2} a_1]$ ist, so ist $[a_1] \geq [2b_1]$. Wenn daher auch noch $[a_2] > [a_1]$ ist, so ist (a_1, b_1, a_2) eine reducirte Form und der Satz bewiesen.

Ist dagegen $[a_2] < [a_1]$, so nehmen wir den absolut kleinsten Rest von $-b_1$ für den Modul a_2; wird dieser Rest b_2 genannt und $\frac{b_2^2 + D}{a_2} = a_3$ gesetzt, so ergiebt sich leicht, dass a_3 eine ganze Zahl ist. Wir bilden dann die dritte Form (a_2, b_2, a_3), und diese ist der vorhergehenden, also auch der gegebenen eigentlich äquivalent. Ausserdem ist $[a_2] \geq [2b_2]$. Wenn also noch $[a_3] > [a_2]$ ist, so ist (a_2, b_2, a_3) eine reducirte Form und der Satz bewiesen.

Ist aber $[a_3] < [a_2]$, so bilden wir auf die dargelegte Art eine vierte, darauf nöthigenfalls eine fünfte Form und fahren in dieser Weise fort, bis wir zu einer Form gelangen, bei welcher der absolute Werth des letzten Coefficienten nicht kleiner als derjenige des ersten ist. Da $[a_2] < [a_1]$, $[a_3] < [a_2], \ldots$ vorausgesetzt wird, so bilden die positiven ganzen Zahlen

$$[a_1],\ [a_2],\ [a_3],\ \ldots$$

eine abnehmende Reihe, und da eine solche nicht unbegrenzt sein kann, so müssen wir nach einer endlichen Reihe von Operationen zu einer Zahl a_{m+1} gelangen, deren absoluter Werth nicht kleiner als derjenige der vorhergehenden Zahl a_m ist. Die Form (a_m, b_m, a_{m+1}) ist dann reducirt und der gegebenen Form (a, b, a_1) eigentlich äquivalent.

Beispiele. I. Um eine der Form (248, 150, 175), deren Determinante -3400 ist, äquivalente reducirte Form zu erhalten, nehmen wir den absolut kleinsten Rest von -150 für den Modul 175; dieser Rest ist $b_1 = 25$. Da nun $\frac{25^2 + 3400}{175} = 23$ ist, so erhalten wir die neue Form (175, 25, 23), welche noch nicht reducirt ist, da $23 < 175$ ist. Wir nehmen also weiter den absolut kleinsten Rest von -25 für den Modul 23; dieser ist -2, und da $\frac{(-2)^2 + 3400}{23} = 148$ ist, so erhalten wir die dritte Form (23, -2, 148); diese ist reducirt.

II. (48, 15, 11), (11, -4, 29). $[-D = -303]$

III. (121, 49, 20), (20, — 9, 5), (5, — 1, 4),
(4, 1, 5). [$-D = -19$].

IV. (75, 33, 26), (26, — 7, 35). [$-D = -861$].

V. (— 200, 100, — 51), (— 51, 2, — 4),
(— 4, ± 2, — 51). [$-D = -200$].

VI. (304, 217, 155), (155, — 62, 25), (25, 12, 7), (7, 2, 5),
(5, — 2, 7). [$-D = -31$].

Anmerkung. Ist (a, b, c) eine reducirte Form, deren Determinante $-D$ ist, so ist $[2b] \leq [a]$, also $4b^2 \leq a^2$. Es ist aber auch $[a] \leq [c]$, also $a^2 \leq ac$ und somit $4b^2 \leq ac$, folglich $3b^2 \leq ac - b^2$, d. i. $3b^2 \leq D$ und

$$[b] \leq \sqrt{\tfrac{1}{3} D}.$$

Ferner ist $ac = D + b^2$, und da, wie wir eben gesehen haben, $b^2 \leq \frac{1}{3} D$ ist, so ist $ac \leq \frac{4}{3} D$. Es ist aber $a^2 \leq ac$, also auch $a^2 \leq \frac{4}{3} D$ und

$$[a] \leq \sqrt{\tfrac{4}{3} D}.$$

§ **108.** Ermittlung aller reducirten Formen einer gegebenen negativen Determinante. — Da die absoluten Werthe der Coefficienten a, b einer reducirten Form (a, b, c), wie wir eben gesehen haben, gewisse Grenzen nicht überschreiten können, und da der Werth des dritten Coefficienten c bestimmt ist, sobald man die Determinante $-D$ und a, b kennt, so ist die Anzahl der reducirten Formen, deren Determinante $-D$ ist, eine endliche.

Um alle diese Formen zu bestimmen, wählt man für b alle, sowohl positiven als negativen Zahlen, deren absoluter Werth nicht grösser als $\sqrt{\frac{1}{3} D}$ ist. Darauf zerlegt man jede Zahl $b^2 + D$ auf alle möglichen Arten in zwei Factoren, von denen jedoch keine dem absoluten Werthe nach $< [2b]$ sein darf, und setzt, wenn die beiden Factoren ungleich sind, denjenigen, welcher den kleineren absoluten Werth hat, gleich a, den anderen gleich c. Auf diese Weise erhält man alle reducirten Formen der Determinante $-D$.

Beispiele I. Für die Determinante $-D = -48$ ist $\sqrt{\frac{1}{3} D} = 4$; wir setzen also der Reihe nach

$$b = 0, \pm 1, \pm 2, \pm 3, \pm 4.$$

Für diese Werthe ist $b^2 + D$ beziehungsweise

$48 = 1 \cdot 48 = 2 \cdot 24 = 3 \cdot 16 = 4 \cdot 12 = 6 \cdot 8$,

$49 = 7 \cdot 7$,

$52 = 4 \cdot 13$,

57 liefert keine brauchbare Zerlegung,

$64 = 8 \cdot 8$.

Es ergeben sich also die 22 reducirten Formen

$$(\pm 1, 0, \pm 48), (\pm 2, 0, \pm 24), (\pm 3, 0, \pm 16),$$
$$(\pm 4, 0, \pm 12), (\pm 6, 0, \pm 8), (\pm 7, 1, \pm 7),$$
$$(\pm 7, -1, \pm 7), (\pm 4, 2, \pm 13), (\pm 4, -2, \pm 13),$$
$$(\pm 8, 4, \pm 8), (\pm 8, -4, \pm 8).$$

II. Für die Determinante -17 ist $2 < \sqrt{\tfrac{1}{3}D} < 3$; wir setzen also der Reihe nach

$$b = 0, \pm 1, \pm 2.$$

Für diese Werthe ist $b^2 + D$ beziehungsweise

$$17 = 1 \cdot 17;\ 18 = 2 \cdot 9 = 3 \cdot 6;\ 21,$$

welche Zahl keine brauchbare Zerlegung liefert. Es ergeben sich also die 10 reducirten Formen

$$(\pm 1, 0, \pm 17), (\pm 2, 1, \pm 9), (\pm 2, -1, \pm 9),$$
$$(\pm 3, 1, \pm 6), (\pm 3, -1, \pm 6).$$

III. $-D = -40$. Reducirte Formen:

$$(\pm 1, 0, \pm 40), (\pm 2, 0, \pm 20), (\pm 4, 0, \pm 10),$$
$$(\pm 5, 0, \pm 8), (\pm 7, 3, \pm 7), (\pm 7, -3, \pm 7).$$

IV. $-D = -85$. Reducirte Formen:

$$(\pm 1, 0, \pm 85), (\pm 5, 0, \pm 17), (\pm 2, 1, \pm 43),$$
$$(\pm 2, -1, \pm 43), (\pm 10, 5, \pm 11), (\pm 10, -5, \pm 11).$$

§ 109. Eigentliche Aequivalenz zweier Formen einer negativen Determinante. — Es seien (a, b, c) und (a', b', c') zwei eigentlich äquivalente Formen der Determinante $-D$, und zwar sollen zunächst beide Formen als reducirte vorausgesetzt werden. Die Substitution, durch welche (a, b, c) in (a', b', c') transformirt wird, sei

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y'. \end{cases}$$

[Man beachte, dass dadurch auch die inverse Substitution, d. h. die Substitution, welche (a', b', c') in (a, b, c) transformirt, bestimmt ist]. Ohne die Allgemeinheit der Betrachtung zu beeinträchtigen, können wir ferner $[a'] \leq [a]$ voraussetzen. Es ist nun nach § 98

$$(1) \qquad a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$

$$(2) \qquad b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$

$$(3) \qquad \alpha\delta - \beta\gamma = +1.$$

Aus (1) folgt durch Multiplication mit a

$$aa' = a^2\alpha^2 + 2ab\alpha\gamma + ac\gamma^2 + b^2\gamma^2 - b^2\gamma^2$$

oder, da

$$ac - b^2 = +D$$

ist,

$$aa' = (a\alpha + b\gamma)^2 + D\gamma^2.$$

Diese Formel lehrt, dass a, a' dasselbe Zeichen haben, und da c dasselbe Zeichen wie a, c' dasselbe Zeichen wie a' hat, so sind die vier Zahlen a, a', c, c' sämmtlich positiv oder sämmtlich negativ.

Da ferner jede der Zahlen $a, a' \leq \sqrt{\frac{4D}{3}}$, also $aa' \leq \frac{4D}{3}$ ist, so muss $D\gamma^2 < \frac{4D}{3}$, also $\gamma^2 < \frac{4}{3}$ sein. Es ist also entweder $\gamma = 0$ oder $\gamma = \pm 1$.

1. Fall. Es sei $\gamma = 0$; dann folgt aus (3), dass $\alpha\delta = +1$, also $\alpha = \delta = \pm 1$ ist, und aus (1) $a' = a\alpha^2 = a$. Ferner geht die Gleichung (2) über in $b' = a\alpha\beta + b$; es muss also $b' - b$ durch $a = a'$ theilbar sein. Nun ist $[b'] \leq [\frac{1}{2}a']$, also auch $\leq [\frac{1}{2}a]$, und $[b]$ ist ebenfalls $\leq [\frac{1}{2}a]$, somit

$$[b' - b] \leq [a],$$

und da $b' - b$ durch a theilbar sein soll, so muss entweder $b' - b = 0$ oder $b' - b = a$ sein.

Wenn $b' - b = 0$, also $b' = b$ ist, so muss, da auch noch $a' = a$ ist, $c' = c$ sein. Beide Formen sind also identisch, in welchem Falle sich die Aequivalenz von selbst versteht.

Wenn dagegen $b' - b = a$ ist, so muss die eine der beiden Zahlen b, b' gleich $+\frac{1}{2}a$, die andere gleich $-\frac{1}{2}a$ sein, da der absolute Werth einer jeden nicht grösser als $[\frac{1}{2}a]$

sein soll. Aus der Gleichheit der Determinanten beider Formen ergiebt sich auch in diesem Falle $c' = c$. Die Formen sind also

$$(a, +\tfrac{1}{2}a, c) \quad \text{und} \quad (a, +\tfrac{1}{2}a, c);$$

beide Formen sind danach ambig und die eine der andern entgegengesetzt.

2. Fall. Für $\gamma = \pm 1$ liefert die Gleichung (1)

$$a' = a\alpha^2 \pm 2b\alpha + c.$$

Da wir nun $|a'| \leq |a|$, also auch $|a'| \leq |c|$ voraussetzen, so kann diese Gleichung nur bestehen, wenn

$$a\alpha^2 \pm 2b\alpha \leq 0 \quad \text{oder} \quad \geq 0$$

ist, je nachdem a', c positive oder negative Zahlen sind. Da aber $|2b| \leq |a|$ und $|\alpha| \leq \alpha^2$, also $|2b\alpha| \leq |a\alpha^2|$ ist, so kann $a\alpha^2 \pm 2b\alpha$ für ein positives a ebenso wenig negativ, wie für ein negatives a positiv sein. Es ist daher

$$a\alpha^2 \pm 2b\alpha = 0,$$

und dann folgt aus dem für a' gefundenen Werthe, dass $a' = c$ ist. Da nun $[a'] \leq [a]$, $[a] \leq [c]$ ist, so muss

$$a = a' = c$$

sein. Mit Rücksicht hierauf geht (1) über in die schon oben erhaltene Formel

$$a\alpha^2 \pm 2b\alpha = 0 \quad \text{oder} \quad \alpha(a\alpha \pm 2b) = 0.$$

Da $|a| \geq |2b|$ ist, so darf, wenn diese Gleichung bestehen soll, $[\alpha]$ nicht > 1 angenommen werden. Es ist also entweder $\alpha = 0$ oder $\alpha = \pm 1$.

Wenn erstens $\alpha = 0$ ist, so folgt aus (3) $\beta\gamma = -1$ und sodann aus (2)

$$b' = -b \pm c\delta.$$

Es ist also $b' + b = \pm c\delta$ durch $c = a$ theilbar, und dann ergiebt sich, ganz wie im 1. Falle, dass entweder

$$b' = b = +\tfrac{1}{2}a \quad \text{oder} \quad b' = -b$$

ist. Beide Formen sind also entweder identisch [jede $(a, \frac{1}{2}a, a)$] oder entgegengesetzt (a, b, a), $(a, -b, a)$.

Ist dagegen zweitens $\alpha = \pm 1$, so folgt aus (1)

$$a \pm 2b = 0.$$

Es ist also $+2b = a = a'$, und dann liefert die Gleichung (2)

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$$

oder, wenn $\alpha\delta$ durch $1 + \beta\gamma$ ersetzt wird,

$$b' = a(\alpha\beta + \gamma\delta) + b(1 + 2\beta\gamma),$$

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma).$$

Es ist also $b' - b$ durch a theilbar, und dann ergiebt sich wie oben, dass entweder $b' = b$, also beide Formen identisch, oder $b' = -b$ und zugleich $b = \pm \frac{1}{2}a$, $b' = \mp \frac{1}{2}a$, also beide Formen entgegengesetzt und zugleich ambig sind.

Wir sehen somit, dass zwei nicht identische reducirte Formen einer negativen Determinante nur in den beiden folgenden Fällen eigentlich äquivalent sind:

1. Beide Formen sind entgegengesetzt und zugleich ambig, also $(a, \frac{1}{2}a, c)$, $(a, -\frac{1}{2}a, c)$.

2. Beide Formen sind entgegengesetzt und haben als ersten und dritten Coefficienten die nämliche Zahl, also (a, b, a), $(a, -b, a)$.

Es ist jetzt leicht zu entscheiden, ob zwei beliebige Formen F, F' derselben negativen Determinante eigentlich äquivalent sind oder nicht. Wir ermitteln nach dem oben dargelegten Verfahren zwei reducirte Formen f, f', welche beziehungsweise F, F' äquivalent sind. Sind diese reducirten Formen identisch oder eigentlich äquivalent, so sind auch die vorgelegten Formen äquivalent, sonst nicht.

Beispiele. I. Sind die Formen (37, 53, 78), (53, 73, 102) der Determinante — 77 äquivalent?

(37, 53, 78), (78, 25, 9), (9, 2, 9).

(53, 73, 102), (102, 29, 9), (9, — 2, 9).

Da (9, 2, 9) und (9, — 2, 9) äquivalent sind, so sind es auch die vorgelegten Formen.

II. Sind die Formen (23, 38, 63), (15, 20, 27) der Determinante — 5 äquivalent?

(23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, 1, 3).

(15, 20, 27), (27, 7, 2), (2, 1, 3).

Da die reducirten Formen identisch sind, so sind die vorgelegten Formen äquivalent.

III. Die Formen (5, 14, 41), (10, 11, 13) der Determinante — 9 sind nicht äquivalent, denn

$$(5,\ 14,\ 41),\ (41,\ -14,\ 5),\ (5,\ -1,\ 2),\ (2,\ 1,\ 5);$$

aber

$$(10,\ 11,\ 13),\ (13,\ 2,\ 1),\ (1,\ 0,\ 9).$$

§ 110. Transformation einer gegebenen Form einer negativen Determinante in eine gegebene äquivalente Form. — Es sind zwei äquivalente Formen (A, B, A_1), (a, b, a_1) derselben Determinante $-D$ gegeben, und es soll eine eigentliche Substitution ermittelt werden, welche die erste in die zweite überführt. Zu diesem Zwecke bilden wir auf die in § 107 dargelegte Weise die Reihe der Formen

$$(A, B, A_1), (A_1, B_1, A_2), \ldots, (A_{m-1}, B_{m-1}, A_m), (A_m, B_m, A_{m+1}),$$

von denen die letzte reducirt ist. Ebenso bilden wir, mit der zweiten Form beginnend, die Reihe

$$(a, b, a_1), (a_1, b_1, a_2), \ldots, (a_{n-1}, b_{n-1}, a_n), (a_n, b_n, a_{n+1}),$$

deren letztes Glied eine reducirte Form ist.

Da die gegebenen Formen äquivalent sind, so müssen die reducirten Formen (A_m, B_m, A_{m+1}), (a_n, b_n, a_{n+1}) entweder identisch, oder entgegengesetzt und zugleich ambig, oder entgegengesetzt und zugleich so beschaffen sein, dass

$$A_m = A_{m+1} = a_n = a_{n+1}$$

ist.

In den beiden ersten Fällen ist die vorletzte Form der ersten Reihe, nämlich (A_{m-1}, B_{m-1}, A_m) der Form

$$(a_n,\ -b_{n-1},\ a_{n-1})$$

nach links benachbart; denn in beiden Fällen ist zunächst $A_m = a_n$. Ferner ist nach der Bildungsweise der Formen

$$B_{m-1} \equiv -B_m \pmod{A_m} \quad \text{und} \quad b_{n-1} \equiv -b_n \pmod{a_n = A_m},$$

also

$$B_{m-1} - b_{n-1} \equiv b_n - B_m \pmod{A_m};$$

die rechte Seite dieser Congruenz ist aber im ersten Falle $\equiv 0$, da dann $b_n = B_m$ ist, und im zweiten Falle ebenfalls $\equiv 0 \pmod{A_m}$, da dann $B_m = +\frac{1}{2} A_m$, $b_n = -\frac{1}{2} A_m$, also $b_n - B_m = -A_m$ ist. In beiden Fällen sind also die ge-

nannten Formen benachbart, und somit ist jede Form der Reihe

$$(A, B, A_1), (A_1, B_1, A_2), \ldots, (A_{m-1}, B_{m-1}, A_m), (a_n, -b_{n-1}, a_{n-1}),$$
$$(a_{n-1}, -b_{n-2}, a_{n-2}), \ldots, (a_1, -b, a), (a, b, a_1)$$

der folgenden nach links benachbart.

Eine Reihe von derselben Beschaffenheit ist

$$(A, B, A_1), (A_1, B_1, A_2), \ldots, (A_m, B_m, A_{m+1}), (a_n, -b_{n-1}, a_{n-1}),$$
$$(a_{n-1}, -b_{n-2}, a_{n-2}), \ldots, (a_1, -b, a), (a, b, a_1),$$

wenn die beiden erhaltenen reducirten Formen entgegengesetzt sind und zugleich $A_m = A_{m+1} = a_n = a_{n+1}$ ist.

In jedem Falle ist also die Ermittlung einer Substitution, durch welche die eine von zwei gegebenen äquivalenten Formen der nämlichen negativen Determinante in die andere übergeführt wird, zurückgeführt auf die Transformation der ersten Form einer Reihe von benachbarten Formen in ein beliebiges anderes Glied dieser Reihe, und diese Aufgabe soll uns jetzt beschäftigen.

Die Reihe der benachbarten Formen sei

$$F, F_1, F_2, \ldots, F_k, \ldots, F_m$$

oder

$$(a, b, a_1), (a_1, b_1, a_2), (a_2, b_2, a_3), \ldots, (a_k, b_k, a_{k+1}), \ldots,$$
$$(a_m, b_m, a_{m+1}),$$

und die unbestimmten Grössen sollen beziehungsweise durch

$$x, y; x_1, y_1; x_2, y_2; \ldots; x_k, y_k; \ldots; x_m, y_m$$

bezeichnet werden. Ferner nehmen wir an, F gehe über in

F_1 durch die Substitution $x = \alpha_1 x_1 + \beta_1 y_1$, $y = \gamma_1 x_1 + \delta_1 y_1$

F_2 " " " $x = \alpha_2 x_2 + \beta_2 y_2$, $y = \gamma_2 x_2 + \delta_2 y_2$

. . . .

F_k " " " $x = \alpha_k x_k + \beta_k y_k$, $y = \gamma_k x_k + \delta_k y_k$

. . . .

Danach wird F in F_{k-1} transformirt, wenn man

$$\begin{cases} x = \alpha_{k-1} x_{k-1} + \beta_{k-1} y_{k-1} \\ y = \gamma_{k-1} x_{k-1} + \delta_{k-1} y_{k-1} \end{cases}$$

setzt; nach § 101 geht aber F_{k-1} in F_k durch die Substitution

$$\begin{cases} x_{k-1} = - y_k \\ y_{k-1} = x_k + h_k y_k \end{cases}$$

über, wo der Kürze wegen

$$h_k = \frac{b_{k-1} + b_k}{a_k}$$

geschrieben ist. Somit verwandelt sich F in F_k durch die Substitution

$$\begin{cases} x = \alpha_{k-1}(-y_k) + \beta_{k-1}(x_k + h_k y_k) \\ y = \gamma_{k-1}(-y_k) + \delta_{k-1}(x_k + h_k y_k) \end{cases}$$

oder, was dasselbe ist,

$$\begin{cases} x = \beta_{k-1} x_k + (h_k \beta_{k-1} - \alpha_{k-1}) y_k \\ y = \delta_{k-1} x_k + (h_k \delta_{k-1} - \gamma_{k-1}) y_k . \end{cases}$$

Nach unserer Voraussetzung ist aber

$$x = \alpha_k x_k + \beta_k y_k , \quad y = \gamma_k x_k + \delta_k y_k$$

die Substitution, welche F in F_k transformirt; somit ist allgemein

$$\begin{cases} \alpha_k = \beta_{k-1} \\ \beta_k = h_k \beta_{k-1} - \alpha_{k-1} \\ \gamma_k = \delta_{k-1} \\ \delta_k = h_k \delta_{k-1} - \gamma_{k-1} . \end{cases}$$

Da $\alpha_{k-1} = \beta_{k-2}$ und $\gamma_{k-1} = \delta_{k-2}$ ist (nach der ersten und dritten dieser Formeln), so lassen sich die Formeln, welche die Werthe von β_k, δ_k liefern, auch folgendermassen schreiben:

$$\beta_k = h_k \beta_{k-1} - \beta_{k-2} ,$$
$$\delta_k = h_k \delta_{k-1} - \delta_{k-2} .$$

Da nach § 101

$$\alpha_1 = 0 , \quad \beta_1 = -1 , \quad \gamma_1 = 1 , \quad \delta_1 = h_1$$

ist, und da die Zahlen h durch die Formeln

$$h_1 = \frac{b + b_1}{a_1} , \quad h_2 = \frac{b_1 + b_2}{a_2} , \; \ldots , \; h_k = \frac{b_{k-1} + b_k}{a_k} , \ldots$$

bestimmt sind, so enthalten obige Formeln die Lösung der gestellten Aufgabe.

Was die Anwendung derselben betrifft, so verfährt man zweckmässig auf folgende Weise:

Man schreibt die Zahlen $h_1, h_2, h_3, \ldots$ in eine Horizontallinie; unter h_1 setzt man $\alpha_1 = 0$, unter h_2 ebenso $\beta_1 = -1$. Darauf multiplicirt man h_2 mit β_1, zieht vom Produkt die vorhergehende Zahl (in diesem Falle $\alpha_1 = 0$) ab und schreibt den Rest unter h_3. So fährt man fort. Man multiplicirt jedes h mit der darunter stehenden Zahl, zieht die vorhergehende Zahl vom Produkt ab und schreibt den Rest daneben. In die folgende Horizontallinie setzt man ebenso $\gamma_1 = 1$ unter h_1, $\delta_1 = h_1$ unter h_2 und verfährt genau wie in der vorhergehenden Horizontallinie. Auf diese Weise kommt zuletzt α_k unter h_k und γ_k unter α_k zu stehen; ferner wird sich β_k neben (rechts von) α_k und δ_k neben γ_k befinden.

Beispiele. I. Die Formen (23, 38, 63), (15, 20, 27) der Determinante -5 sind äquivalent; man soll die erste in die zweite transformiren. Die erste Form liefert die Reihe

(23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, 1, 3),

die zweite die Reihe

$$(15, 20, 27),\quad (27, 7, 2),\quad (2, 1, 3).$$

Die Endglieder beider Reihen sind identisch; wir bilden also die Reihe der benachbarten Formen

$$(23, 38, 63),\ (63, 25, 10),\ (10, 5, 3),\ (3, 1, 2),$$
$$(2, -7, 27),\ (27, -20, 15),\ (15, 20, 27)$$

und transformiren die erste in die letzte.

Es ist hier

$$h_1 = \frac{38+25}{63} = 1,\quad h_2 = \frac{25+5}{10} = 3,\quad h_3 = \frac{5+1}{3} = 2,$$

$$h_4 = \frac{1-7}{2} = -3,\ h_5 = \frac{-7-20}{27} = -1,\ h_6 = \frac{-20+20}{15} = 0,$$

also

$h_1 = 1$	$h_2 = 3$	$h_3 = 2$	$h_4 = -3$	$h_5 = -1$	$h_6 = 0$	
0	-1	-3	-5	18	-13	-18
1	1	2	3	-11	8	$+11$

Die gesuchte Substitution ist demnach

$$\begin{cases} x = -13x' - 18y' \\ y = \quad 8x' + 11y'. \end{cases}$$

II. Eine eigentliche Transformation der Form (3, — 3, 17) in die äquivalente Form (59, 28, 14) zu ermitteln.

Die erste Form liefert die Reihe

$$(3, -3, 17), \quad (17, 3, 3), \quad (3, 0, 14),$$

die zweite die Reihe

$$(59, 28, 14), \quad (14, 0, 3), \quad (3, 0, 14).$$

Wir haben also die erste Form der Reihe

$$(3, -3, 17), \quad (17, 3, 3), \quad (3, 0, 14),$$
$$(14, -28, 59), \quad (59, 28, 14)$$

in die letzte zu transformiren. Es ergiebt sich

$h_1 = 0$	$h_2 = 1$	$h_3 = -2$	$h_4 = 0$	
0	-1	-1	3	1
1	0	-1	2	1.

Die gesuchte Substitution ist also

$$\begin{cases} x = 3x' + y' \\ y = 2x' + y'. \end{cases}$$

Wenn die Formen (A, B, A_1) und (a, b, a_1) uneigentlich äquivalent sind, so sind (A, B, A_1) und $(a, -b, a_1)$ eigentlich äquivalent. Wir können also eine eigentliche Substitution

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases}$$

ermitteln, welche (A, B, A_1) in $(a, -b, a_1)$ transformirt. Dann geht aber durch die Substitution

$$\begin{cases} x = \alpha x' - \beta y' \\ y = \gamma x' - \delta y' \end{cases}$$

offenbar (A, B, A_1) in (a, b, a_1) über. Diese letztere Substitution ist eine uneigentliche; denn da

$$\alpha\delta - \beta\gamma = +1$$

sein soll, so ist

$$-\alpha\delta + \beta\gamma = -1.$$

Wenn demnach zwei uneigentlich äquivalente Formen gegeben sind, so lässt sich eine uneigentliche Substitution ermitteln, welche die eine in die andere transformirt, und wenn

die gegebenen Formen sowohl eigentlich, als auch uneigentlich äquivalent sind, so kann man eine eigentliche und auch eine uneigentliche Transformation der einen in die andere bestimmen.

Beispiel. Die Formen (18, 32, 57) und (17, — 24, 34) der Determinante — 2 sind auf beide Arten äquivalent. Wenn wir eine eigentliche Transformation der ersten in die zweite suchen, so führt das oben dargelegte Verfahren zu der Reihe der benachbarten Formen

$$(18, 32, 57),\ (57, 25, 11),\ (11, -3, 1),\ (1, -1, 3),$$
$$(3, 10, 34),\ (34, 24, 17),\ (17, -24, 34).$$

Es ergiebt sich also

$h_1 = 1$	$h_2 = 2$	$h_3 = -4$	$h_4 = 3$	$h_5 = 1$	$h_6 = 0$	
0	-1	-2	9	29	20	-29
1	1	1	-5	-16	-11	16

und die gesuchte eigentliche Substitution ist

$$\begin{cases} x = 20x' - 29y' \\ y = -11x' + 16y'. \end{cases}$$

Um zweitens eine uneigentliche Transformation von (18, 32, 57) in (17, — 24, 34) zu erhalten, ermitteln wir eine eigentliche Transformation von (18, 32, 57) in (17, 24, 34). Wir erhalten die Reihe der benachbarten Formen

$$(18, 32, 57),\ (57, 25, 11),\ (11, -3, 1),\ (1, 1, 3),$$
$$(3, -10, 34),\ (34, -24, 17),\ (17, 24, 34),$$

und daraus ergiebt sich

$h_1 = 1$	$h_2 = 2$	$h_3 = -2$	$h_4 = -3$	$h_5 = -1$	$h_6 = 0$	
0	-1	-2	5	-13	8	13
1	1	1	-3	8	-5	-8.

(18, 32, 57) wird also in (17, 24, 34) durch die eigentliche Substitution

$$\begin{cases} x = 8x' + 13y' \\ y = -5x' - 8y' \end{cases}$$

und somit in $(17, -24, 34)$ durch die uneigentliche Substitution

$$\begin{cases} x = 8x' - 13y' \\ y = -5x' + 8y' \end{cases}$$

transformirt.

§ 111. Auflösung der Pell'schen Gleichung und Darstellungen einer Zahl durch eine Form. — Nachdem wir eine eigentliche Transformation der gegebenen Form $F = (a, b, c)$ in die äquivalente Form F' erhalten haben, müssen wir, um alle übrigen gleichartigen Substitutionen, welche F in F' überführen, zu ermitteln, die Gleichung

$$t^2 - (b^2 - ac)u^2 = m^2,$$

in welcher m den grössten gemeinschaftlichen Divisor von a, $2b$, c bezeichnet, in ganzen Zahlen auflösen. Wenn wir die Determinante der Form F mit $-D$ bezeichnen, so ist D eine positive Zahl, und die Gleichung geht über in

$$t^2 + Du^2 = m^2. \tag{1}$$

Nun ist

$$4D = 4ac - (2b)^2,$$

also

$$\frac{4D}{m^2} = \frac{4ac}{m^2} - \left(\frac{2b}{m}\right)^2,$$

und da m in a, $2b$, c aufgeht, so wird $\frac{4D}{m^2}$ eine ganze Zahl sein. Wenn nun

1. $\frac{4D}{m^2} > 4$, also $D > m^2$ ist, so hat die Gleichung (1) offenbar nur die beiden Lösungen $t = \pm m$, $u = 0$. Ist

2. $\frac{4D}{m^2} = 4$, also $D = m^2$, so erhalten wir die 4 Lösungen

t	m	$-m$	0	0
u	0	0	1	-1

3. Wenn $\frac{4D}{m^2} = 3$, also $4D = 3m^2$ ist, so muss m eine gerade Zahl sein, und wir erhalten die 6 Lösungen

t	m	$-m$	$\frac{1}{2}m$	$\frac{1}{2}m$	$-\frac{1}{2}m$	$-\frac{1}{2}m$
u	0	0	1	-1	1	-1

4. Wenn $\frac{4D}{m^2} = 2$, d. h. $\frac{4ac}{m^2} = 2 + \left(\frac{2b}{m}\right)^2$ ist, so wird

$$\left(\frac{2b}{m}\right)^2 \equiv -2 \equiv 2 \pmod{4}$$

sein. Da aber keine Quadratzahl, durch 4 dividirt, den Rest 2 giebt, so ist dieser Fall unmöglich. Ebenso wenig kann

5. $\frac{4D}{m^2} = 1$ sein; denn dann müsste

$$\left(\frac{2b}{m}\right)^2 = -1 + \frac{4ac}{m^2}, \quad \text{also} \quad \left(\frac{2b}{m}\right)^2 \equiv -1 \equiv 3 \pmod{4}$$

sein, welche Congruenz ebenfalls unmöglich ist.

Da nun D weder $= 0$ noch negativ sein kann, so sind hiermit alle Fälle erschöpft.

Wenn also $F = (a, b, c)$ durch die Substitution

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases}$$

in

$$F' = \left(M, v, \frac{v^2 + D}{M}\right)$$

übergeht und $\frac{4D}{m^2} > 4$ ist, so ist

$$\begin{cases} x = -\alpha x' - \beta y' \\ y = -\gamma x' - \delta y' \end{cases}$$

die einzige gleichartige Substitution, die es giebt, und es gehören somit zur Wurzel v der Congruenz

$$\xi^2 \equiv -D \pmod{M}$$

nur die beiden eigentlichen Darstellungen

$$x = \pm \alpha, \qquad y = \pm \gamma$$

der Zahl M durch die Form (a, b, c).

Wenn zweitens $\frac{4D}{m^2} = 4$ ist, so erhalten wir ausser den beiden genannten noch zwei Transformationen, nämlich

$$\begin{cases} x = \mp \frac{1}{m}(b\alpha + c\gamma)x' \mp \frac{1}{m}(b\beta + c\delta)y' \\ y = \pm \frac{1}{m}(a\alpha + b\gamma)x' \pm \frac{1}{m}(a\beta + b\delta)y', \end{cases}$$

also noch zwei weitere zur Wurzel v gehörende eigentliche Darstellungen, nämlich

$$\begin{cases} x = \mp \frac{1}{m}(b\alpha + c\gamma) \\ y = \pm \frac{1}{m}(a\alpha + b\gamma). \end{cases}$$

Wenn endlich $\frac{4D}{m^2} = 3$ ist, so giebt es 6 gleichartige Transformationen von F in F', nämlich ausser den beiden für den ersten Fall geltenden noch

$$\begin{cases} x = \left[\pm \frac{1}{2}\alpha \mp \frac{1}{m}(b\alpha + c\gamma)\right]x' \\ \quad + \left[\pm \frac{1}{2}\beta \mp \frac{1}{m}(b\beta + c\delta)\right]y' \\ y = \left[\pm \frac{1}{2}\gamma \pm \frac{1}{m}(a\alpha + b\gamma)\right]x' \\ \quad + \left[\pm \frac{1}{2}\delta \pm \frac{1}{m}(a\beta + b\delta)\right]y' \end{cases}$$

und

$$\begin{cases} x = \left[\pm \frac{1}{2}\alpha \pm \frac{1}{m}(b\alpha + c\gamma)\right]x' \\ \quad + \left[\pm \frac{1}{2}\beta \pm \frac{1}{m}(b\beta + c\delta)\right]y' \\ y = \left[\pm \frac{1}{2}\gamma \mp \frac{1}{m}(a\alpha + b\gamma)\right]x' \\ \quad + \left[\pm \frac{1}{2}\delta \mp \frac{1}{m}(a\beta + b\delta)\right]y', \end{cases}$$

denen die vier weiteren, zu v gehörigen eigentlichen Darstellungen

$$\begin{cases} x = \pm \frac{1}{2}\alpha \mp \frac{1}{m}(b\alpha + c\gamma) \\ y = \pm \frac{1}{2}\gamma \pm \frac{1}{m}(a\alpha + b\gamma) \end{cases}$$

und

$$\begin{cases} x = \pm \frac{1}{2}\alpha \pm \frac{1}{m}(b\alpha + c\gamma) \\ y = \pm \frac{1}{2}\gamma \mp \frac{1}{m}(a\alpha + b\gamma) \end{cases}$$

entsprechen.

Beispiel. Es soll die Primzahl 227 durch die Form $(3, -3, 17)$, deren Determinante -42 ist, dargestellt werden.

Die Congruenz $\xi^2 \equiv -42 \pmod{227}$ hat die beiden

Wurzeln ± 56. Wir nehmen zuerst $v = +56$ und untersuchen, ob die gegebene Form äquivalent

$$\left(227, 56, \frac{56^2 + 42}{227} = 14\right)$$

ist. Wir erhalten die beiden Reihen

$$(3, -3, 17),\ (17, 3, 3),\ (3, 0, 14),$$
$$(227, 56, 14),\ (14, 0, 3),\ (3, 0, 14).$$

Da die erhaltenen reducirten Formen identisch sind, so findet eigentliche Aequivalenz statt, und um eine Transformation zu ermitteln, bilden wir die Reihe der benachbarten Formen

$$(3, -3, 17),\ (17, 3, 3),\ (3, 0, 14),$$
$$(14, -56, 227),\ (227, 56, 14).$$

Es ergiebt sich

$h_1 = 0$	$h_2 = 1$	$h_3 = -4$	$h_4 = 0$	
0	-1	-1	5	1
1	0	-1	4	1.

Wir erhalten also die Substitution

$$x = 5x' + y',\quad y = 4x' + y'.$$

Da nun $m = 1$, $D = 42$, also $\frac{4D}{m^2} > 4$ ist, so sind

$$x = \pm 5,\quad y = \pm 4$$

die einzigen zur Wurzel $+56$ gehörenden eigentlichen Darstellungen der Zahl 227 durch die Form $(3, -3, 17)$.

Die Ermittlung der zu $v = -56$ gehörenden eigentlichen Darstellungen führt zu der Reihe

$$(3, -3, 17),\ (17, 3, 3),\ (3, 0, 14),$$
$$(14, 56, 227),\ (227, -56, 14).$$

Es ist also

$h_1 = 0$	$h_2 = 1$	$h_3 = 4$	$h_4 = 0$	
0	-1	-1	-3	1
1	0	-1	-4	1,

und die so bestimmten Substitutionen liefern die beiden Darstellungen $x = \pm 3$, $y = \pm 4$.

Aufgabe. Alle eigentlichen Darstellungen der Zahl 205 durch die Form (5, — 5, 30) zu ermitteln.

$$|x = \pm 5, \quad y = \pm 1$$

und

$$x = \pm 7, \quad y = \pm 1|.$$

Uneigentliche Darstellungen. — Wir setzen jetzt voraus, eine Zahl M sei durch eine Form $F = (a, b, c)$ vermittels solcher Werthe x_1, y_1 dargestellt, die nicht prim zu einander sind, und zwar sei $x_1 = m\xi$, $y_1 = m\eta$, wo m der grösste gemeinschaftliche Divisor von x_1 und y_1 ist, so dass also ξ, η relative Primzahlen sind. Dann geht die Gleichung

$$M = ax_1^2 + 2bx_1y_1 + cy_1^2$$

über in

$$M = m^2(a\xi^2 + 2b\xi\eta + c\eta^2);$$

also ist M durch m^2 theilbar, und es ist

$$x = \xi, \quad y = \eta$$

eine eigentliche Darstellung der Zahl $\frac{M}{m^2}$ durch die Form (a, b, c).

Wenn demnach M durch keine Quadratzahl theilbar ist, so giebt es auch keine uneigentlichen Darstellungen dieser Zahl.

Wenn dagegen M einen oder mehrere quadratische Factoren, z. B. m^2, n^2, ..., enthält, so bestimmen wir nach dem Früheren die eigentlichen Darstellungen der Zahl $\frac{M}{m^2}$ durch die Form F. Werden die für die unbestimmten Grössen erhaltenen Werthe mit m multiplicirt, so erhält man diejenigen Darstellungen von M durch F, bei welchen die Werthe von x, y den grössten gemeinschaftlichen Divisor m haben.

Ebenso suchen wir weiter die eigentlichen Darstellungen der Zahl $\frac{M}{n^2}$ durch F und multipliciren die für x, y erhaltenen Werthe mit n, u. s. w.

Danach sind z. B.

$$\begin{cases} x = \pm 10 \\ y = \pm 8 \end{cases} \quad \text{und} \quad \begin{cases} x = \pm 6 \\ y = \pm 8 \end{cases}$$

die uneigentlichen Darstellungen der Zahl $908 = 4 . 227$ durch die Form $(3, -3, 17)$. [Da die Congruenz

$$\xi^2 \equiv -42 \pmod{908}$$

unmöglich ist, so giebt es keine eigentliche Darstellung von 908 durch $(3, -3, 17)$].

§ 112. Darstellung der Zahlen als Summe zweier Quadrate. — Um die erhaltenen Resultate anzuwenden, behandeln wir die Zerlegung der Zahlen in zwei Quadrate. Dabei beschränken wir uns der Einfachheit halber auf ungerade Zahlen und auf solche Zerlegungen $x^2 + y^2$, bei denen x und y prim zu einander sind. Da die Form $F = x^2 + y^2$ die Determinante -1 hat, so muss, wenn eine Zahl M durch F darstellbar sein soll, -1 quadratischer Rest von M sein. Wenn also M eine Primzahl ist, so muss diese die Form $4n + 1$ haben, und wenn die Zahl M zusammengesetzt ist, so muss jeder ihrer Primfactoren von der Form $4n + 1$ sein. Ist diese Bedingung erfüllt, so ist die Congruenz

$$\xi^2 \equiv -1 \pmod{M}$$

immer möglich und hat 2^k Wurzeln $\pm v$, $\pm v'$, ..., wenn k die Anzahl der verschiedenen in M enthaltenen ungeraden Primzahlen bezeichnet.

Um nun die zur Wurzel v gehörenden Darstellungen von M zu erhalten, bilden wir die Form

$$F' = \left(M, v, \frac{v^2 + 1}{M}\right).$$

Da $F = (1, 0, 1)$ die einzige reducirte Form der Determinante -1 ist, so ist F' jedenfalls äquivalent F und somit die Darstellung möglich. Um dieselbe zu ermitteln, transformiren wir F in F'. Geschieht das durch die Substitution

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y', \end{cases}$$

so sind $x = \pm \alpha$, $y = \pm \gamma$ zwei zum Werthe v des Ausdrucks $\sqrt{-1} \pmod{M}$ gehörende Darstellungen. Da aber hier $m = 1$, $D = 1$, also $\frac{4D}{m^2} = 4$ ist, so sind noch zwei weitere zu v gehörende Darstellungen, nämlich

$$x = \mp \gamma, \quad y = \pm \alpha$$

vorhanden. Es giebt also 4 zur Wurzel v gehörende Darstellungen.

Die zum entgegengesetzten Werthe $-v$ gehörenden Darstellungen führen zu der Form

$$F''' = \left(M, -v, \frac{v^2+1}{M}\right),$$

die gleichfalls F äquivalent sein wird. Da nun die Transformation von F in F''' offenbar durch die Substitution

$$\begin{cases} x = \quad \alpha x' - \beta y' \\ y = -\gamma x' + \delta y' \end{cases}$$

erfolgt, so erhalten wir die vier zu $-v$ gehörenden Darstellungen

$$\begin{cases} x = \pm \alpha \\ y = \mp \gamma \end{cases}, \quad \begin{cases} x = \pm \gamma \\ y = \pm \alpha . \end{cases}$$

Diese 8 verschiedenen Darstellungen von M durch F, die zu den Wurzeln $\pm v$ der Congruenz

$$\xi^2 \equiv -1 \pmod{M}$$

gehören, liefern aber nur eine Zerfällung von M in zwei Quadrate, wenn man bloss die Grösse dieser Quadrate, nicht ihre Reihenfolge und die Vorzeichen ihrer Wurzeln berücksichtigt.

Wenn M eine Primzahl ist, so hat die Congruenz

$$\xi^2 \equiv -1 \pmod{M}$$

keine Wurzeln ausser $\pm v$; somit sind in diesem Falle auch nur die 8 angegebenen Darstellungen von M durch die Form $(1, 0, 1)$ möglich, und wir gelangen zu dem berühmten (von Fermat gefundenen, aber erst von Euler in den Nov. Comm. Petrop. V bewiesenen) Satze:

Jede (positive) Primzahl von der Form $4n+1$ lässt sich, und zwar nur auf eine Weise, als Summe zweier Quadrate darstellen.

Wenn M noch einen zweiten Primfactor (der auch die Form $4n+1$ haben muss) enthält, so hat die Congruenz

$$\xi^2 \equiv -1 \pmod{M}$$

noch ein zweites Paar entgegengesetzter Wurzeln $\pm v'$, welche eine zweite Zerlegung von M in zwei Quadrate liefern.

Enthält M 3 Primfactoren, so hat die Congruenz

$$\xi^2 \equiv -1 \pmod{M},$$

wie wir oben gesehen haben, 2^3 Wurzeln, also 2^2 Paare entgegengesetzter Wurzeln, so dass sich 4 Zerlegungen von M ergeben.

Wenn M allgemein k ungleiche Primfactoren enthält, so hat die Congruenz $\xi^2 \equiv -1 \pmod{M}$ nach § 80 2^k Wurzeln, also 2^{k-1} Paare entgegengesetzter Wurzeln; folglich lässt sich M auf 2^{k-1} Arten als Summe zweier Quadrate darstellen. [Vergleiche auch § 37 und 83].

Beispiele. I. Es sei $M = 653$. Die Congruenz

$$\xi^2 \equiv -1 \pmod{653}$$

hat die Wurzeln ± 149, und wir müssen eine reducirte Form suchen, welche $\left(653,\ 149,\ \frac{149^2+1}{653} = 34\right)$ äquivalent ist.

$$(653, 149, 34),\quad (34, -13, 5),\quad (5, -2, 1),\quad (1, 0, 1).$$

Wir haben also das erste Glied der Reihe

$$(1, 0, 1),\quad (1, 2, 5),\quad (5, 13, 34),$$
$$(34, -149, 653),\quad (653, 149, 34)$$

in das letzte zu transformiren. Es ergiebt sich

$h_1 = 2$	$h_2 = 3$	$h_3 = -4$	$h_4 = 0$	
0	-1	-3	13	3
1	2	5	-22	-5

,

und somit ist

$$653 = 13^2 + 22^2.$$

II. $$M = 85 = 5 \cdot 17.$$

Die Congruenz $\xi^2 \equiv -1 \pmod{85}$ hat die vier Wurzeln ± 13, ± 38.

1. $(85, 13, 2)$, $(2, 1, 1)$, $(1, 0, 1)$.

$$(1, 0, 1),\quad (1, -1, 2),\quad (2, -13, 85),\quad (85, 13, 2).$$

$h_1 = -1$	$h_2 = -7$	$h_3 = 0$	
0	-1	7	1
1	-1	6	1

.

Darstellung: $85 = 7^2 + 6^2$.

2. (85, 38, 17), (17, — 4, 1), (1, 0, 1).

(1, 0, 1), (1, 4, 17), (17, — 38, 85), (85, 38, 17).

$h_1 = 4$	$h_2 = -2$	$h_3 = 0$	
0	— 1	2	1
1	4	— 9	— 4

Darstellung: $85 = 2^2 + 9^2$.

III. $M = 13949 = 13 . 29 . 37$.

Die Congruenz $\xi^2 \equiv -1 \pmod{13949}$ hat die 8 Wurzeln ± 1955, ± 2917, ± 4594, ± 5556.

1. (13949, 1955, 274), (274, — 37, 5),
(5, 2, 1), (1, 0, 1).

(1, 0, 1), (1, — 2, 5), (5, 37, 274), (274, — 1955, 13949),
(13949, 1955, 274).

$h_1 = -2$	$h_2 = 7$	$h_3 = -7$	$h_4 = 0$	
0	— 1	— 7	50	7
1	— 2	— 15	107	15

Darstellung: $13949 = 50^2 + 107^2$.

2. (13949, 2917, 610), (610, 133, 29), (29, 12, 5),
(5, — 2, 1), (1, 0, 1).

(1, 0, 1), (1, 2, 5), (5, — 12, 29), (29, — 133, 610),
(610, — 2917, 13949), (13949, 2917, 610).

$h_1 = 2$	$h_2 = -2$	$h_3 = -5$	$h_4 = -5$	$h_5 = 0$	
0	— 1	2	— 9	43	9
1	2	— 5	23	— 110	— 23

Darstellung: $13949 = 43^2 + 110^2$.

3. (13949, 4594, 1513), (1513, — 55, 2),
(2, 1, 1), (1, 0, 1).

(1, 0, 1), (1, — 1, 2), (2, 55, 1513),
(1513, — 4594, 13949), (13949, 4594, 1513).

$h_1 = -1$	$h_2 = 27$	$h_3 = -3$	$h_4 = 0$	
0	-1	-27	82	27
1	-1	-28	85	28

Darstellung: $13949 = 82^2 + 85^2$.

4. (13949, 5556, 2213), (2213, 1083, 530), (530, − 23, 1), (1, 0, 1).

(1, 0, 1), (1, 23, 530), (530, − 1083, 2213), (2213, − 5556, 13949), (13949, 5556, 2213).

$h_1 = 23$	$h_2 = -2$	$h_3 = -3$	$h_4 = 0$	
0	-1	2	-5	-2
1	23	-47	118	47

Darstellung: $13949 = 5^2 + 118^2$.

Anwendung der Zerfällung einer Zahl in zwei Quadrate. — Die Darstellung der Zahlen als Summe zweier Quadrate benutzt Euler (Commentationes Algebr. Collectae, T. I p. 167) zur Lösung der Aufgabe:

„Zu untersuchen, ob eine gegebene Zahl der Form $4n + 1$ eine Primzahl sei oder nicht."

Ergiebt sich nämlich, dass eine Zahl der Form $4n + 1$ auf keine Weise in zwei Quadrate zerfällt werden kann, so ist sie sicherlich zusammengesetzt, und zwar enthält sie (eine gerade Anzahl von) Primfactoren der Form $4n + 3$.

Kann die Zahl nur auf eine Weise als Summe zweier Quadrate dargestellt werden, so ist sie eine Primzahl.

Sind endlich mehrere Zerfällungen der Zahl in zwei Quadrate möglich, so ist dieselbe zusammengesetzt und zwar aus Primfactoren der Form $4n + 1$.

Es kommt also darauf an, die gegebene Zahl M auf alle möglichen Arten in zwei Quadrate zu zerlegen. Zu diesem Zwecke subtrahirt Euler von M alle Quadratzahlen, die $< M$ sind, und zwar beginnt er mit der grössten derselben. So oft der Rest gleichfalls eine Quadratzahl ist, liegt eine Zerlegung von M in zwei Quadrate vor.

Die gegebene Zahl kann auf 1, 3, 7 oder 9 endigen (der Fall, in welchem sie auf 5 endigt, kann unberücksichtigt bleiben, da eine solche Zahl immer zusammengesetzt ist). Da nun keine Quadratzahl auf 2, 3, 7, 8 endigen kann, so können diejenigen Quadrate, welche Reste dieser Endungen liefern würden, weggelassen werden. Es brauchen also von der gegebenen Zahl nur diejenigen Quadrate subtrahirt zu werden, welche Reste mit den Endungen 0, 1, 4, 5, 6, 9 geben.

Wenn demnach die Zahl auf 1 endigt, so endigen die zu subtrahirenden Quadrate auf 0, 1, 5, 6, ihre Wurzeln also auf 0, 1, 4, 5, 6, 9. Betrachten wir ebenso die anderen Endungen, die stattfinden können, so erhalten wir folgende Tabelle:

Endung der Zahl	der zu subtrahirenden Quadrate	der Wurzeln dieser Quadrate
1	0, 1, 5, 6.	0, 1, 4, 5, 6, 9.
3	4, 9.	2, 3, 7, 8.
7	1, 6.	1, 4, 6, 9.
9	0, 4, 5, 9.	0, 2, 3, 5, 7, 8.

Für jede vorgelegte Zahl sind danach so viele Operationen vorzunehmen, als passende Wurzelendungen vorhanden sind (wenn die Zahl auf 1 oder 9 endigt, 6; wenn dieselbe auf 3 oder 7 endigt, 4).

Ist p^2 das erste (grösste) zu subtrahirende Quadrat, so ist das zweite Quadrat derselben Endung $(p - 10)^2$, das dritte $(p - 20)^2$, u. s. w. Diese Subtractionen lassen sich nun leicht durch Additionen ersetzen.

Es ist nämlich

$$M - (p - 10)^2 = M - p^2 + 20p - 100.$$

Hat man also $M - p^2$ bestimmt, so braucht man zum Rest nur $20p - 100$ zu addiren, um $M - (p - 10)^2$ zu erhalten. Addirt man zu dem jetzt erhaltenen Rest $20p - 300$, so erhält man

$$M - p^2 + 40p - 400 = M - (p - 20)^2, \text{ u. s. w.}$$

Nach Bildung der ersten Differenz $M - p^2$ hat man also der Reihe nach

$$20p - 100, \quad 20p - 300, \quad 20p - 500, \ldots.$$

(eine arithmetische Progression mit der Differenz — 200) zu addiren und bei jeder Summe nachzusehen, ob dieselbe ein Quadrat sei oder nicht.

Diese Reihe von Operationen hat man aber nur so weit fortzusetzen, bis man zur Hälfte der gegebenen Zahl gelangt; denn wenn eine Zahl $M = 4n + 1$ sich in zwei Quadrate zerfällen lässt, so ist das eine gewiss $> \frac{1}{2} M$.

Beispiele. 1. Zu untersuchen, ob 27541 eine Primzahl sei oder nicht.

27541	27541	27541
$165^2 = 27225$	$164^2 = 26896$	$161^2 = 25921$
316	645	1620
3200	3180	3120
3516	3825	4740
3000	2980	2920
6516	6805	7660
2800	2780	2720
9316	9585	10380
2600	2580	2520
11916	12165	12900
2400	2380	2320
14316	14545	15220

27541	27541	27541
$160^2 = 25600$	$159^2 = 25281$	$156^2 = 24336$
1941	2260	3205
3100	3080	3020
□ 5041	5340	6225
2900	2880	2820
7941	8220	9045
2700	2680	2620
10641	10900	11665
2500	2480	2420
13141	13380	14085

Da sich nur die eine Zerlegung

$$27541 = 150^2 + 71^2$$

ergiebt, so ist 27541 eine Primzahl.

II. Zu untersuchen, ob 212237 eine Primzahl sei oder nicht.

212237	212237	212237	212237
$459^2 = 210681$	$456^2 = 207936$	$454^2 = 206116$	$451^2 = 203401$
1556	4301	6121	□ 8836
9080	9020	8980	8920
10636	13321	15101	17756
8880	8820	8780	8720
19516	22141	23881	26476
8680	8620	8580	8520
28196	30761	32461	34996
8480	8420	8380	8320
36676	39181	40841	43316
8280	8220	8180	8120
44956	47401	49021	51436
8080	8020	7980	7920
53036	55421	57001	59356
7880	7820	7780	7720
60916	63241	64781	67076
7680	7620	7580	7520
68596	70861	□ 72361	74596
7480	7420	7380	7320
76076	78281	79741	81916
7280	7220	7180	7120
83356	85501	86921	89036
7080	7020	6980	6920
90436	92521	93901	95956
6880	6820	6780	6720
97316	99341	100681	102676
6680	6620	6580	6520
103996	105961	107261	109196
6480			
110476			

Da sich die beiden Zerlegungen

$$212237 = 374^2 + 269^2 = 451^2 + 94^2$$

ergeben, so besteht 212237 aus 2 Factoren.

Wenn sich für eine Zahl mehrere Zerlegungen in zwei

Quadrate ergeben haben, so ist es auch leicht, diese Zahl in ihre Factoren zu zerlegen.

Es sei

$$M = a^2 + b^2 = c^2 + d^2 .$$

Wir dürfen $a > b$, $c > d$ und, da die Zerlegungen verschieden sein sollen, auch $a > c$, folglich $b < d$ voraussetzen. Wird

$$a = c + x, \quad d = b + y$$

angenommen, so geht die Gleichung

$$a^2 + b^2 = c^2 + d^2$$

über in

$$(1) \qquad x^2 + 2cx = y^2 + 2by .$$

Da die eine Seite dieser Gleichung durch x, die andere durch y theilbar ist, so wollen wir

$$x^2 + 2cx = y^2 + 2by = xyz$$

setzen, wo z auch ein Bruch sein kann. Dann ergiebt sich

$$c = \frac{yz - x}{2}, \quad b = \frac{xz - y}{2},$$

also

$$a = \frac{yz + x}{2}, \quad d = \frac{xz + y}{2}$$

und

$$(2) \qquad M = a^2 + b^2 = \frac{(x^2 + y^2)(1 + z^2)}{4} .$$

Wenn beide Zahlen a, c gerade oder ungerade sind, so ist offenbar $x^2 + y^2$ durch 4 theilbar; ist dagegen eine der Zahlen a, c gerade, die andere ungerade, so ist $x^2 + y^2$ durch 2 theilbar. Es folgt also aus der Gleichung (2), dass M theilbar ist durch einen Divisor einer der drei Zahlen

$$x^2 + y^2, \quad \frac{x^2 + y^2}{2}, \quad \frac{x^2 + y^2}{4} .$$

Nun liefert die Gleichung (1)

$$\frac{x}{y} = \frac{y + 2b}{x + 2c} = \frac{b + d}{a + c} .$$

Dieser Bruch, in den kleinsten Zahlen ausgedrückt, sei $\frac{p}{q}$. Dann ist nothwendig eine der drei Zahlen

$$p^2 + q^2, \quad \tfrac{1}{2}(p^2 + q^2), \quad \tfrac{1}{4}(p^2 + q^2)$$

ein Divisor von M.

Man übersehe nicht, dass die Zahlen a, b, c, d als Quadratwurzeln das Zeichen $\pm$ haben.

Um z. B. die Divisoren der oben untersuchten Zahl 212237 zu finden, setzen wir

$$a = \pm 451, \qquad b = \pm 94,$$
$$c = \pm 374, \qquad d = \pm 269.$$

Dann ist

$$b + d = \pm 363 \quad \text{oder} \quad = \pm 175,$$
$$a + c = \pm 825 \quad \text{oder} \quad = \pm 77.$$

Da es sich nur um den absoluten Werth der Zahlen handelt, so können wir von den Zeichen abstrahiren und erhalten

$$\frac{b+d}{a+c} = \frac{363}{825} = \frac{11}{25} \quad \text{oder} = \frac{363}{77} = \frac{33}{7},$$

und da

$$11^2 + 25^2 = 746, \quad 7^2 + 33^2 = 1138$$

ist, so sind

$$\tfrac{1}{2}(746) = 373 \quad \text{und} \quad \tfrac{1}{2}(1138) = 569$$

die Divisoren von 212237.

§ 113. Darstellung der Zahlen als Summe eines Quadrats und eines doppelten Quadrats. — Wenn eine Zahl M durch die Form $(1, 0, 2)$, welche die Determinante -2 hat, darstellbar sein soll, so muss -2 quadratischer Rest von M sein. Also darf die Zahl M, die wieder als ungerade vorausgesetzt wird, nach § 84 nur Primfactoren der beiden Formen $8n + 1$, $8n + 3$ enthalten. Wenn diese Bedingung erfüllt ist, so ist die Congruenz

$$\xi^2 \equiv -2 \pmod{M}$$

stets möglich und hat 2^k Wurzeln $\pm v$, $\pm v', \ldots$, wo k die Anzahl der verschiedenen Primfactoren von M bezeichnet.

Wir bilden jetzt die Form

$$F' = \left(M, v, \frac{v^2+2}{M}\right).$$

Da dieselbe die Determinante -2 hat, und da es für diese Determinante nur die eine reducirte Form $F = (1, 0, 2)$ giebt, so werden F und F' jedenfalls äquivalent sein; die Darstellung von M durch F ist also möglich.

Um dieselbe zu erhalten, suchen wir die eigentlichen

Transformationen von F in F'. Da $m = 1$, $D = 2$, also $\frac{4D}{m^2} > 4$ ist, so giebt es nur zwei solcher Transformationen, nämlich

$$\begin{cases} x = \pm \alpha x' \pm \beta y' \\ y = \pm \gamma x' \pm \delta y', \end{cases}$$

und daher auch nur zwei zur Wurzel v gehörende Darstellungen

$$x = \pm \alpha, \quad y = \pm \gamma$$

der Zahl M durch die Form (1, 0, 2).

Weiter findet man, dass zu dem Werthe $-v$ des Ausdrucks $\sqrt{-2}$ (mod. M) die beiden Darstellungen $x = \pm \alpha$, $y = \mp \gamma$ gehören. Die 4 Darstellungen, die zu dem Wurzelpaar $\pm v$ gehören, liefern aber, wenn man nur auf die Grösse der Quadrate sieht, nur die eine Zerlegung der Zahl M

$$M = \alpha^2 + 2\gamma^2.$$

Ist demnach M eine Primzahl, so ist die erhaltene Zerlegung die einzige dieser Art, die möglich ist, und wir erhalten so den schon Fermat bekannten, aber erst von Lagrange bewiesenen Satz:

Jede Primzahl einer der beiden Formen $8n + 1$, $8n + 3$ kann, und zwar nur auf eine Weise, in ein Quadrat und das Doppelte eines Quadrats zerfällt werden.

Ist M eine zusammengesetzte Zahl, so liefert das zweite Paar entgegengesetzter Wurzeln $\pm v'$ der Congruenz

$$\xi^2 \equiv -2 \text{ (mod. } M)$$

eine zweite Zerlegung von M. Allgemein erhalten wir, wenn M aus k ungleichen Primfactoren besteht, 2^{k-1} verschiedene Zerlegungen.

Beispiele. I. Es sei $M = 587$. Die Congruenz

$$\xi^2 \equiv -2 \text{ (mod. } 587)$$

hat die beiden Wurzeln ± 207.

$$(587,\ 207,\ 73),\ \ (73,\ 12,\ 2),\ \ (2,\ 0,\ 1),\ \ (1,\ 0,\ 2).$$

$$(1,\ 0,\ 2),\ \ (2,\ -12,\ 73),$$

$$(73,\ -207,\ 587),\ \ (587,\ 207,\ 73).$$

$h_1 = -6$	$h_2 = -3$	$h_3 = 0$	
0	-1	3	1
1	-6	17	6

Zerlegung: $587 = 3^2 + 2 \cdot 17^2$.

II. $M = 4579 = 241 \cdot 19$.

Die Congruenz $\xi^2 \equiv -2 \pmod{4579}$ hat die 4 Wurzeln ± 203, ± 279.

1. $(4579, 203, 9)$, $(9, 4, 2)$, $(2, 0, 1)$, $(1, 0, 2)$.
$(1, 0, 2)$, $(2, -4, 9)$, $(9, -203, 4579)$, $(4579, 203, 9)$.

$h_1 = -2$	$h_2 = -23$	$h_3 = 0$	
0	-1	23	1
1	-2	45	2

Zerlegung: $4579 = 23^2 + 2 \cdot 45^2$.

2. $(4579, 279, 17)$, $(17, -7, 3)$, $(3, 1, 1)$, $(1, 0, 2)$.
$(1, 0, 2)$, $(2, 0, 1)$, $(1, -1, 3)$, $(3, 7, 17)$,
$(17, -279, 4579)$, $(4579, 279, 17)$.

$h_1 = 0$	$h_2 = -1$	$h_3 = 2$	$h_4 = -16$	$h_5 = 0$	
0	-1	1	3	-49	-3
1	0	-1	-2	33	2

Zerlegung: $4579 = 49^2 + 2 \cdot 33^2$.

§ 114. Weitere Zerlegungen. — Da es für die Determinante -3 zwei reducirte Formen giebt, nämlich $(1, 0, 3)$ und $(2, 1, 2)$, so kann jede Zahl, für welche -3 quadratischer Rest ist, durch eine dieser beiden Formen dargestellt werden, und zwar so, dass die Werthe von x und y prim zu einander sind. Nun ist nach § 85 die Zahl -3 Rest aller Primzahlen $12n + 1$ und $12n + 7$, d. h. aller Primzahlen $3n + 1$, und die Form $(2, 1, 2)$ kann offenbar nur gerade Zahlen darstellen. Wenn wir den Gegenstand ganz in derselben Weise, wie es oben für die Form $(1, 0, 2)$ geschah, weiter verfolgen, so erhalten wir den zuerst von Euler bewiesenen Satz:

Jede Primzahl von der Form $3n + 1$ lässt sich, und zwar nur auf eine Weise, in ein Quadrat und das Dreifache eines Quadrats zerfällen.

Beispiel. Es sei $M = 829$.

Die Congruenz $\xi^2 \equiv -3 \pmod{829}$ hat die Wurzeln ± 251.

$$(829, 251, 76), \ (76, -23, 7), \ (7, 2, 1), \ (1, 0, 3).$$
$$(1, 0, 3), \ (3, 0, 1), \ (1, -2, 7), \ (7, 23, 76),$$
$$(76, -251, 829), \ (829, 251, 76).$$

$h_1 = 0$	$h_2 = -2$	$h_3 = 3$	$h_4 = -3$	$h_5 = 0$	
0	-1	2	7	-23	-7
1	0	-1	-3	10	3

Zerlegung: $829 = 23^2 + 3 \cdot 10^2$.

Wenn M eine zusammengesetzte ungerade Zahl ist, so ist die Congruenz $\xi^2 \equiv -3 \pmod{M}$ nur möglich, wenn jede der k Primzahlen, welche M enthält, die Form $3n + 1$ hat. Ist diese Bedingung erfüllt, so hat jene Congruenz 2^k Wurzeln, von denen je zwei $(\pm v)$ eine Zerlegung liefern, so dass sich im Ganzen 2^{k-1} Zerlegungen ergeben.

Für die Determinante -5 giebt es zwei nicht äquivalente reducirte Formen, nämlich $(1, 0, 5)$ und $(2, 1, 3)$. Durch eine dieser Formen lässt sich also jede Zahl M darstellen, für welche -5 quadratischer Rest ist. Für jeden Primfactor p von M muss dann also $\left(\frac{-5}{p}\right)$, d. i. $\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$ den Werth $+1$ haben. Dies ist der Fall, wenn erstens

$$\left(\frac{-1}{p}\right) = +1, \quad \text{also} \quad p = 4m + 1$$

und zugleich $\left(\frac{5}{p}\right)$, d. i.

$$\left(\frac{p}{5}\right) = +1, \quad \text{also} \quad p = \pm 1 + 5n$$

ist. Vereinigt man diese beiden Bedingungen, so erhält man als Formen der Primzahlen, für welche -5 quadratischer Rest ist, zunächst

$$20n + 1 \quad \text{und} \quad 20n + 9.$$

Das Symbol $\left(\frac{-5}{p}\right)$ hat aber auch zweitens den Werth $+1$, wenn gleichzeitig

$$\left(\frac{-1}{p}\right) = -1\,, \quad \text{also} \quad p = 4m + 3$$

und $\left(\frac{5}{p}\right)$, d. i.

$$\left(\frac{p}{5}\right) = -1\,, \quad \text{also} \quad p = 5n + 2$$

ist, und durch Vereinigung dieser beiden Bedingungen erhält man weiter

$$20n + 3 \quad \text{und} \quad 20n + 7$$

als Formen der Primzahlen, für welche -5 quadratischer Rest ist.

[Man beachte, dass für die Primzahlen $20n + 1$, $20n + 9$ zugleich -5 und $+5$ Reste sind, während für die Primzahlen $20n + 3$, $20n + 7$ nur -5 Rest ist].

Es lassen sich also alle Zahlen M, deren Primfactoren von einer der vier genannten Formen sind, durch eine der beiden Formen (1, 0, 5), (2, 1, 3) darstellen.

Im vorliegenden Falle ist es nun auch leicht zu entscheiden, durch welche dieser beiden Formen die Zahl M sich wird darstellen lassen. Es sei zunächst

$$M = x^2 + 5y^2\,,$$

so ist $x^2 \equiv M$ (mod. 5), also M quadratischer Rest von 5.

Ist dagegen

$$M = 2x^2 + 2xy + 3y^2\,,$$

so ist

$$\begin{aligned} 2M = 4x^2 + 4xy + 6y^2 &= (2x + y)^2 + 5y^2 \\ &\equiv (2x + y)^2 \text{ (mod. 5)}\,, \end{aligned}$$

also $2M$ Rest von 5, und da 2 Nichtrest ist, so wird auch M Nichtrest von 5 sein. Wir sehen somit, dass jede Zahl M, welche eine der Formen $20n + 1$, $20n + 9$ hat, durch die Form (1, 0, 5) darstellbar ist, während jede Zahl M, welche von einer der Formen $20n + 3$, $20n + 7$ ist, durch die Form (2, 1, 3) dargestellt werden kann.

Was nun die Darstellung der Zahlen durch die Form (1, 0, 5) betrifft, so sei k die Anzahl der in M enthaltenen ungleichen Primzahlen; dann besitzt die Congruenz

$$\xi^2 \equiv -5 \pmod{M}$$

2^k Wurzeln $\pm v$, $\pm v'$, ... Da ferner $m = 1$, $\frac{4D}{m^2} > 4$ ist, so giebt es nur zwei Substitutionen

$$\begin{cases} x = \pm \alpha x' \pm \beta y' \\ y = \pm \gamma x' \pm \delta y', \end{cases}$$

welche (1, 0, 5) in $\left(M, v, \frac{v^2+5}{M}\right)$ transformiren, und diese beiden liefern nur die eine Zerlegung

$$x = \pm \alpha, \qquad y = \pm \gamma.$$

Auch die Form $\left(M, -v, \frac{v^2+5}{M}\right)$ führt zu keiner neuen Zerlegung, da sie aus (1, 0, 5) durch die Substitution

$$\begin{cases} x = \pm \alpha x' \mp \beta y' \\ y = \pm \gamma x' \mp \delta y' \end{cases}$$

erhalten wird. Da somit je zwei Wurzeln $\pm v$ nur eine Zerlegung geben, so kann die Zahl M auf 2^{k-1} Arten in ein Quadrat und das Fünffache eines Quadrats zerfällt werden.

Für den Fall $k = 1$ folgt hieraus der Satz:

Jede Primzahl einer der beiden Formen $20n + 1$, $20n + 9$ kann und zwar nur auf eine Weise in ein Quadrat und das Fünffache eines Quadrats zerlegt werden.

Beispiele. I. $p = 89$.

Die Congruenz $\xi^2 \equiv -5 \pmod{89}$ hat die Wurzeln ± 23.

(1, 0, 5), (5, 0, 1), (1, − 1, 6), (6, − 23, 89), (89, 23, 6).

$h_1 = 0$	$h_2 = -1$	$h_3 = -4$	$h_4 = 0$	
0	− 1	1	− 3	− 1
1	0	− 1	4	1

Zerlegung: $89 = 3^2 + 5 \cdot 4^2$.

II. $M = 192821 = 29 \cdot 61 \cdot 109$.

$\xi^2 \equiv -5 \pmod{192821}$ hat die 8 Wurzeln ± 35277, ± 61873, ± 63726, ± 90322, von denen jedes Paar eine Zerlegung liefert.

1. Zerlegung.

(1, 0, 5), (5, 0, 1), (1, — 5, 30), (30, — 205, 1401),
(1401, 3007, 6454), (6454, — 35277, 192821),
(192821, 35277, 6454).

$h_1 = 0$	$h_2 = -5$	$h_3 = -7$	$h_4 = 2$	$h_5 = -5$	$h_6 = 0$	
0	− 1	5	− 34	− 73	399	73
1	0	− 1	7	15	− 82	−15

Zerlegung: $192821 = 399^2 + 5 \cdot 82^2$.

2. Zerlegung.

(1, 0, 5), (5, 0, 1), (1, 2, 9),
(9, — 20, 45), (45, 110, 269),
(269, 2311, 19854), (19854, — 61873, 192821),
(192821, 61873, 19854).

$h_1 = 0$	$h_2 = 2$	$h_3 = -2$	$h_4 = 2$	$h_5 = 9$	$h_6 = -3$	$h_7 = 0$	
0	− 1	− 2	5	12	103	−321	−103
1	0	− 1	2	5	43	−134	− 43

Zerlegung: $192821 = 321^2 + 5 \cdot 134^2$.

3. Zerlegung.

(1, 0, 5), (5, 0, 1), (1, 3, 14), (14, 543, 21061),
(21061, — 63726, 192821), (192821, 63726, 21061).

$h_1 = 0$	$h_2 = 3$	$h_3 = 39$	$h_4 = -3$	$h_5 = 0$	
0	− 1	− 3	− 116	351	116
1	0	− 1	− 39	118	39

Zerlegung: $192821 = 351^2 + 5 \cdot 118^2$.

4. Zerlegung.

(1, 0, 5), (5, 0, 1), (1, — 1, 6), (6, — 11, 21),
(21, 53, 134), (134, — 321, 769),
(769, 5704, 42309), (42309, — 90322, 192821),
(192821, 90322, 42309).

$h_1 = 0$	$h_2 = -1$	$h_3 = -2$	$h_4 = 2$
0	-1	1	-1
1	0	-1	2

$h_5 = -2$	$h_6 = 7$	$h_7 = -2$	$h_8 = 0$	
-3	7	52	-111	-52
5	-12	-89	190	89

Zerlegung: $192821 = 111^2 + 5 \,.\, 190^2$.

III. $M = 989 = 23 \,.\, 43$.

Wurzeln der Congruenz $\xi^2 \equiv -5 \pmod{989}$ sind ± 77, ± 353.

Zerlegungen:

$$989 = 12^2 + 5 \,.\, 13^2,$$
$$989 = 3^2 + 5 \,.\, 14^2.$$

Aehnlich verhält es sich mit der Darstellung der Zahlen durch die Form (2, 1, 3). Auch für diese Form ist

$$m = 1, \quad \frac{4D}{m^2} > 4;$$

also giebt es nur zwei Substitutionen

$$\begin{cases} x = \pm \alpha x' + \beta y' \\ y = \pm \gamma x' + \delta y', \end{cases}$$

welche (2, 1, 3) in $\left(M, v, \frac{v^2+5}{M}\right)$ transformiren, und diesen Substitutionen entsprechen die beiden Darstellungen $x = \pm \alpha$, $y = \pm \gamma$. Zwei andere Darstellungen liefert die zweite Wurzel $-v$; wir erhalten demnach doppelt so viele Darstellungen, als Wurzeln vorhanden sind. Für den Fall, dass M eine Primzahl ist, ergiebt sich also der Satz: **Jede Primzahl einer der beiden Formen $20n + 3$, $20n + 7$ kann auf vier verschiedene Arten durch die Form (2, 1, 3) dargestellt werden.**

Beispiele. I. $M = 83$.

Die Congruenz $\xi^2 \equiv -5 \pmod{83}$ hat die Wurzeln ± 24.

1. $(2, 1, 3), \ (3, -1, 2), \ (2, 3, 7),$
$(7, -24, 83), \ (83, 24, 7).$

$h_1 = 0$	$h_2 = 1$	$h_3 = -3$	$h_4 = 0$	
0	-1	-1	4	1
1	0	-1	3	1

Zerlegungen:

$$83 = 2 \,.\, 4^2 + 2 \,.\, 4 \,.\, 3 + 3 \,.\, 3^2,$$
$$83 = 2 \,.\, (-4)^2 + 2 \,.\, (-4) \,.\, (-3) + 3 \,.\, (-3)^2.$$

2. $(2, 1, 3), \ (3, -1, 2), \ (2, -3, 7),$
$(7, 24, 83), \ (83, -24, 7).$

$h_1 = 0$	$h_2 = -2$	$h_3 = 3$	$h_4 = 0$	
0	-1	2	7	-2
1	0	-1	-3	1

Zerlegungen: $83 = 2 \,.\, 7^2 + 2 \,.\, 7 \,.\, (-3) + 3 \,.\, (-3)^2,$
$83 = 2 \,.\, (-7)^2 + 2 \,.\, (-7) \,.\, 3 + 3 \,.\, 3^2.$

II. $M = 4087 = 61 \,.\, 67.$

Die Congruenz $\xi^2 \equiv -5 \pmod{4087}$ hat die 4 Wurzeln $\pm 751, \ \pm 1689.$

Zerlegungen:

$$\begin{aligned} 4087 &= 2 \,.\, (\mp 49)^2 + 2 \,.\, (\mp 49)(\pm 11) + 3(\pm 11)^2 \\ &= 2 \,.\, (\pm 38)^2 + 2 \,.\, (\pm 38)(\pm 11) + 3(\pm 11)^2 \\ &= 2 \,.\, (\pm 17)^2 + 2 \,.\, (\pm 17)(\pm 29) + 3(\pm 29)^2 \\ &= 2 \,.\, (\mp 46)^2 + 2 \,.\, (\mp 46)(\pm 29) + 3(\pm 29)^2. \end{aligned}$$

Wir überlassen es dem Leser, weitere Zerlegungen zu versuchen.

Zehntes Kapitel.

Quadratische Formen mit positiver nichtquadratischer Determinante.

§ 115. Reducirte Formen. — Wir haben uns weiter mit den Formen zu beschäftigen, deren Determinante D eine positive Zahl ist. Wenn diese Determinante dabei eine Quadratzahl ist, so gestaltet sich die Sache viel einfacher, als im entgegengesetzten Falle. Die Formen mit quadratischer Determinante sollen den Gegenstand des folgenden Kapitels bilden; hier setzen wir voraus, dass D keine Quadratzahl, also $\sqrt{D}$ irrational sei.

Die erste Aufgabe, die wir nun nach § 106 zu lösen haben, ist, zu untersuchen, unter welchen Bedingungen zwei gegebene Formen der nämlichen Determinante äquivalent sind. Auch hier vergleichen wir die vorgelegten Formen nicht direkt mit einander, sondern bilden erst neue, den vorgelegten beziehungsweise äquivalente Formen, die wir nach Gauss gleichfalls reducirte Formen nennen, obschon sie von ganz anderer Natur, wie diejenigen sind, denen wir im Falle negativer Determinanten diesen Namen beigelegt haben.

Eine Form (a, b, a_1) einer positiven nichtquadratischen Determinante $D = b^2 - aa_1$ heisst reducirt, wenn b positiv und $< \sqrt{D}$ ist, und wenn zugleich der absolute Werth von a zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ liegt.

Lehrsatz. Für jede Form $F = (a, b, a_1)$ einer positiven nichtquadratischen Determinante $D = b^2 - aa_1$ giebt es eine äquivalente reducirte Form.

Beweis. Da D keine Quadratzahl sein soll, so muss sowohl a, als auch a_1 von Null verschieden sein. Wir nehmen

jetzt denjenigen Rest von $-b$ für den Modul a_1, der zwischen $\sqrt{D}$ und $\sqrt{D} - |a_1|$ liegt, wo $|a_1|$ den absoluten Werth von a_1 bezeichnet. Da das Intervall von $\sqrt{D} - [a_1]$ bis $\sqrt{D}$ genau $[a_1]$ auf einander folgende Zahlen enthält, so wird sich immer ein, aber auch nur ein solcher Rest für $-b$ ergeben. Diesen Rest nennen wir b_1 und setzen $\frac{b_1^2 - D}{a_1} = a_2$. Da $b_1^2 \equiv b^2$, also $b_1^2 - D \equiv b^2 - D \equiv aa_1 \equiv 0 \pmod{a_1}$ ist, so wird a_2 eine ganze Zahl sein, und wenn wir jetzt die neue Form $F_1 = (a_1, b_1, a_2)$ bilden, so ist dieselbe der Form $F = (a, b, a_1)$ nach rechts benachbart, also eigentlich äquivalent. Wenn nun noch $|a_2| > |a_1|$ ist, so ist, wie wir unten beweisen werden, F_1 eine reducirte Form.

Ist dagegen $|a_2| < [a_1]$, so wählen wir weiter denjenigen Rest von $-b_1$ in Beziehung auf den Modul a_2, der zwischen $\sqrt{D}$ und $\sqrt{D} - |a_2|$ liegt. Wird dieser eindeutig bestimmte Rest b_2 genannt und $\frac{b_2^2 - D}{a_2} = a_3$ gesetzt, so erkennt man wieder, dass a_3 eine ganze Zahl ist, und dass die Form $F_2 = (a_2, b_2, a_3)$ der Form F_1 (weil nach rechts benachbart) und somit auch der Form F äquivalent ist. Ist jetzt $|a_3| > |a_2|$, so ist F_2 die Form, von der wir beweisen werden, dass sie eine reducirte ist. Im entgegengesetzten Falle, bilden wir, in der dargelegten Weise fortfahrend, eine vierte, fünfte, u. s. w. Form, bis wir zu einer Form $F_m = (a_m, b_m, a_{m+1})$ gelangen, in welcher $[a_{m+1}| > [a_m]$ ist. Dies muss endlich einmal geschehen; denn da b_1 zwischen $\sqrt{D}$ und $\sqrt{D} - [a_1|$, also b_1^2 zwischen D und $D + a_1^2 - 2[a_1]\sqrt{D}$ liegt, so wird $b_1^2 - D$ zwischen 0 und $a_1^2 - 2[a_1]\sqrt{D}$ liegen. Der absolute Werth von $b_1^2 - D$ ist daher $< a_1^2$, und somit ist

$$\left[\frac{b_1^2 - D}{a_1}\right], \text{ d. i. } |a_2] < \left[\frac{a_1^2}{a_1}\right], \text{ d. i. } [a_1].$$

Die ganzen positiven Zahlen $[a_1|$, $[a_2]$, ... bilden also eine abnehmende Reihe, und da eine solche nicht unbegrenzt sein kann, so muss einmal ein Glied $[a_{m+1}]$ auftreten, welches nicht kleiner als das vorhergehende $[a_m]$ ist.

Wir haben jetzt noch zu beweisen, dass die Form

$$F_m = (a_m, b_m, a_{m+1}),$$

in welcher auch diese letzte Bedingung erfüllt ist, wirklich reducirt sei. Zu diesem Zwecke zeigen wir erstens, dass $b_m < \sqrt{D}$ ist.

Da b_m zwischen $\sqrt{D}$ und $\sqrt{D} - [a_m]$ liegt, so ist jede der Grössen

$$p = \sqrt{D} - b_m, \; q = b_m - \sqrt{D} + [a_m]$$

und somit auch der Ausdruck $r = q^2 + 2pq + 2p\sqrt{D}$, für welchen sich leicht $D + a_m^2 - b_m^2$ ergiebt, eine positive Zahl. Wird jetzt D durch $b_m^2 - a_m a_{m+1}$ ersetzt, so wird die positive Zahl $r = a_m^2 - a_m a_{m+1}$. Da aber $[a_{m+1}] \geq [a_m]$ ist, so kann der letzte Ausdruck für r nur dann positiv werden, wenn $a_m a_{m+1}$ negativ ist, d. h. wenn a_m, a_{m+1} entgegengesetzte Zeichen haben. Dann ist aber

$$b_m^2 = D + a_m a_{m+1} < D,$$

also $[b_m] < \sqrt{D}$.

Zweitens haben wir darzuthun, dass b_m eine positive Zahl ist. Es ist $- a_m a_{m+1} = D - b_m^2$, also $[a_m] \cdot [a_{m+1}] < D$, und da $[a_m] \leqq [a_{m+1}]$ ist, gewiss $[a_m] < \sqrt{D}$. Folglich ist $\sqrt{D} - [a_m]$ eine positive Zahl, und da b_m zwischen $\sqrt{D} - [a_m]$ und $\sqrt{D}$ liegt, so muss auch b_m positiv sein.

Was endlich $[a_m]$ betrifft, so ist $\sqrt{D} - [a_m]$, wie wir eben gesehen haben, positiv. Folglich ist um so mehr $\sqrt{D} + b_m - [a_m]$ eine positive Zahl, also $[a_m] < \sqrt{D} + b_m$. Andererseits ist $\sqrt{D} - b_m - [a_m] = - q$ negativ, also

$$[a_m] > \sqrt{D} - b_m.$$

$[a_m]$ liegt daher zwischen $\sqrt{D} - b_m$ und $\sqrt{D} + b_m$.

Die Form $F_m = (a_m, b_m, a_{m+1})$ ist somit reducirt, und da jede der Formen

$$F, F_1, F_2, \ldots, F_m$$

der folgenden nach links benachbart ist, so ist jede der folgenden, also auch die erste der letzten eigentlich äquivalent.

Beispiele. I. Um für die Form $(11, 15, 12)$ der Determinante $D = 93$ eine reducirte Form zu bilden, beachten wir, dass $\sqrt{93} = 9, \ldots$ und $\sqrt{93} - 12 = -2, \ldots$ ist. Von den

12 Zahlen des Intervalls von -2 bis $+9$ incl. ist nur die Zahl $9 \equiv -15 \pmod{12}$. Wir setzen also $b_1 = 9$. Da nun $\frac{9^2 - 93}{12} = -1$ ist, so erhalten wir die der gegebenen äquivalente Form $(12, 9, -1)$. Diese Form ist zwar schon reducirt*); wir wollen aber die Reihe der Operationen fortsetzen, bis eine Form (a_m, b_m, a_{m+1}) erscheint, in welcher $|a_{m+1}|$ nicht mehr $< |a_m|$ ist. Die neuen Grenzen für den mittleren Coefficienten sind $\sqrt{93} = 9, \ldots$ und $\sqrt{93} - 1 = 8, \ldots$ Da nun $-9 \equiv 9 \pmod{1}$ und $\frac{9^2 - 93}{-1} = 12$ ist, so erhalten wir die Form $(-1, 9, 12)$, die allen Anforderungen entspricht. Die Reihe der benachbarten Formen ist in diesem Beispiel also

$$(11, 15, 12), (12, 9, -1), (-1, 9, 12).$$

II. $(67, 97, 140), (140, -97, 67), (67, -37, 20),$

$$(20, -3, -1), (-1, 5, 4) \cdot [D = 29).$$

III. $$(28, 9, -2), (-2, 11, 8) \cdot [D = 137].$$

IV. $(17, 2, -2), (-2, 6, 1), (1, 6, -2) \cdot [D = 38]$.

§ 116. Eigenschaften der reducirten Formen. —

Lehrsatz I. **In jeder reducirten Form (a, b, a_1) haben a und a_1 entgegengesetzte Zeichen.**

Beweis. Da $b^2 - aa_1 = D$, also $aa_1 = b^2 - D$ und $b < \sqrt{D}$ ist, so ist aa_1 eine negative Zahl, d. h. a und a_1 haben entgegengesetzte Zeichen.

Lehrsatz II. Der absolute Werth von a_1 liegt ebenso wie der von a zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$; es ist also auch (a_1, b, a) eine reducirte Form.

Beweis. Da $-a_1 = \frac{D - b^2}{a}$ ist und $|a|$ zwischen $\sqrt{D} - b$ und $\sqrt{D} + b$ liegt, so muss $|a_1|$ zwischen $\frac{D - b^2}{\sqrt{D} - b} = \sqrt{D} + b$

*) Wenn wir das dargelegte Verfahren so oft anwenden, bis wir auf eine Form (a_m, b_m, a_{m+1}) stossen, in welcher $|a_{m+1}| > |a_m|$ ist, so haben wir sicher eine reducirte Form gewonnen. Da aber der Begriff der reducirten Form durchaus nicht die Erfüllung der Bedingung $|a_{m+1}| > |a_m|$ fordert, so kann recht gut auch schon früher eine reducirte Form auftreten, und das ist hier der Fall.

und $\frac{D - b^2}{\sqrt{D} + b} = \sqrt{D} - b$ liegen. Wenn dies aber der Fall ist, so erfüllt auch (a_1, b, a) alle Bedingungen einer reducirten Form.

Zusatz. Wenn (a, b, a_1) eine reducirte Form ist, so sind auch (a_1, b, a), $(-a, b, -a_1)$, $(-a_1, b, -a)$ reducirte Formen.

Lehrsatz III. Ist (a, b, a_1) eine reducirte Form, so ist sowohl $[a]$, als auch $[a_1] < 2\sqrt{D}$.

Beweis. Da sowohl $[a]$, als auch $[a_1] < \sqrt{D} + b$ und $b < \sqrt{D}$ ist, so ist um so mehr sowohl $[a]$, als auch $[a_1] < 2\sqrt{D}$.

Lehrsatz IV. Der mittlere Coefficient b einer reducirten Form (a, b, a_1) liegt zwischen $\sqrt{D}$ und $\sqrt{D} - [a]$ und ebenso zwischen $\sqrt{D}$ und $\sqrt{D} - [a_1]$.

Beweis. Da

$$\sqrt{D} + b > [a] > \sqrt{D} - b > 0$$

ist, so ist

$$[a] - \sqrt{D} + b, \text{ d. i. } b - \{\sqrt{D} - [a]\} > 0$$

und $b - \sqrt{D} < 0$; folglich liegt b zwischen $\sqrt{D} - [a]$ und $\sqrt{D}$.

Ganz ebenso beweist man, dass b zwischen $\sqrt{D}$ und $\sqrt{D} - [a_1]$ liegt.

Lehrsatz V. Für jede reducirte Form (a, b, a_1) giebt es eine, aber auch nur eine nach rechts benachbarte Form, welche ebenfalls reducirt ist, und ebenso eine einzige nach links benachbarte reducirte Form.

Beweis. Wir nehmen denjenigen Rest von $-b$ für den Modul a_1, der zwischen $\sqrt{D}$ und $\sqrt{D} - [a_1]$ liegt, nennen denselben b_1, setzen sodann $\frac{b_1^2 - D}{a_1} = a_2$ und bilden die neue Form (a_1, b_1, a_2), so ist dieselbe eindeutig bestimmt und der gegebenen Form (a, b, a_1) nach rechts benachbart. Es bleibt uns also nur zu beweisen, dass (a_1, b_1, a_2) auch reducirt ist.

Da nach Lehrsatz II $[a_1] < \sqrt{D} + b$ ist, so ist

$$p = \sqrt{D} + b - [a_1]$$

eine positive Zahl. Nach demselben Satze ist $[a_1] > \sqrt{D} - b$, also die Zahl

$$q = [a_1] - \{\sqrt{D} - b\}$$

gleichfalls positiv. Endlich ist auch

$$r = \sqrt{D} - b$$

positiv. Wird weiter

$$q_1 = b_1 - \{\sqrt{D} - |a_1|\}$$

und

$$r_1 = \sqrt{D} - b_1$$

gesetzt, so sind auch q_1, r_1 positive Zahlen, da b_1 zwischen $\sqrt{D}$ und $\sqrt{D} - |a_1|$ liegt. Endlich ist $b + b_1 \equiv 0 \pmod{a_1}$, also $b + b_1 = \pm m a_1 = m\,|a_1|$, wo m eine ganze Zahl ist.

Nun ergiebt sich leicht $p + q_1 = b + b_1$, und da $p + q_1$ als Summe zweier positiven Zahlen positiv ist, so muss auch $b + b_1$, folglich auch m positiv sein; es ist also $m - 1$ sicherlich nicht negativ, und dies wird uns den Beweis ermöglichen, dass b_1 eine positive Zahl sei. Es ist nämlich

$$r + q_1 = -b + b_1 + |a_1|.$$

Wenn wir hierzu die Gleichung

$$m\,|a_1| - |a_1| = b + b_1 - |a_1|$$

addiren, so erhalten wir

$$r + q_1 + (m - 1)\,|a_1| = 2 b_1 .$$

Da die linke Seite dieser Gleichung positiv ist, so muss auch $2 b_1$ und somit auch b_1 eine positive Zahl sein, und da b_1 zwischen $\sqrt{D}$ und $\sqrt{D} - |a_1|$ liegt, so ist gewiss $b_1 < \sqrt{D}$, also die zweite Bedingung gleichfalls erfüllt.

Es bleibt noch zu beweisen, dass $|a_1|$ zwischen $\sqrt{D} - b_1$ und $\sqrt{D} + b_1$ liegt. Es ist

$$r + m\,|a_1| = \sqrt{D} + b_1 ,$$

also

$$r + (m - 1)\,|a_1| = \sqrt{D} + b_1 - |a_1|,$$

und da die linke Seite dieser Formel positiv ist, so muss

$$|a_1| < \sqrt{D} + b_1$$

sein. Es ist aber auch

$$q_1 = |a_1| - \{\sqrt{D} - b_1\}$$

eine positive Zahl und somit $|a_1| > \sqrt{D} - b_1$.

Die Form (a_1, b_1, a_2) ist daher reducirt.

Genau ebenso beweist man, dass, wenn man unter b_{-1}

denjenigen Rest von $-b$ in Beziehung auf den Modul a versteht, der zwischen $\sqrt{D}$ und $\sqrt{D} - |a|$ liegt, und $\frac{b_{-1}^2 - D}{a} = a_{-1}$ setzt, die eindeutig bestimmte Form (a_{-1}, b_{-1}, a), welche der gegebenen Form nach links benachbart ist, eine reducirte sein wird.

Beispiele. I. Für die reducirte Form $(2, 4, -6)$ der Determinante 28 erhält man als nach rechts und nach links benachbarte reducirte Formen beziehungsweise $(-6, 2, 4)$ und $(-6, 4, 2)$.

II. $(5, 4, -9)$, $(-9, 5, 4)$, $(4, 7, -3)$ $[D = 61]$.

III. $(-5, 9, 4)$, $(4, 7, -13)$, $(-13, 6, 5)$ $[D = 101]$.

IV. $(3, 9, -7)$, $(-7, 5, 11)$, $(11, 6, -6)$ $[D = 102]$.

§ 117. Ermittlung aller reducirten Formen einer positiven nichtquadratischen Determinante. — Auch die Anzahl der reducirten Formen einer positiven nichtquadratischen Determinante ist eine endliche, da die Coefficienten solcher Formen gewisse Grenzen nicht überschreiten können.

Um für eine gegebene Determinante D alle reducirten Formen (a, b, a_1) zu erhalten, nehme man für b alle positiven Zahlen, die $< \sqrt{D}$ sind, und zerlege für jeden erhaltenen Werth von b den Ausdruck $b^2 - D$ auf alle möglichen Arten in je zwei Factoren von der Beschaffenheit, dass der absolute Werth eines jeden zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ liegt. Wird der eine dieser Factoren a, der andere a_1 genannt, so erhält man die eine Hälfte der reducirten Formen; die andere Hälfte ergiebt sich durch Vertauschung von a und a_1.

Beispiel. Wenn $D = 89$, also $\sqrt{D} = 9, \ldots$ ist, so erhält man für $b = 1, 2, 3, \ldots, 9$ beziehungsweise

$\sqrt{D}+b$	$\sqrt{D}-b$	b^2-D	
$=10,\ldots$	$=8,\ldots$	$=-88$	keine passende
$=11,\ldots$	$=7,\ldots$	$=-85$	Zerlegung
$=12,\ldots$	$=6,\ldots$	$=-80=-(8.10)$	
$=13,\ldots$	$=5,\ldots$	$=-73$	keine Zerlegung
$=14,\ldots$	$=4,\ldots$	$=-64=-(8.8)$	
$=15,\ldots$	$=3,\ldots$	$=-53$	keine Zerlegung
$=16,\ldots$	$=2,\ldots$	$=-40=-(4.10)=-(5.8)$	
$=17,\ldots$	$=1,\ldots$	$=-25=-(5.5)$	
$=18,\ldots$	$=0,\ldots$	$=-8=-(1.8)=-(2.4).$	

Es ergeben sich somit die 24 reducirten Formen

$$(\pm 8, 3, \mp 10), (\pm 10, 3, \mp 8), (\pm 8, 5, \mp 8),$$
$$(\pm 4, 7, \mp 10), (\pm 10, 7, \mp 4), (\pm 5, 7, \mp 8),$$
$$(\pm 8, 7, \mp 5), (\pm 5, 8, \mp 5), (\pm 1, 9, \mp 8),$$
$$(\pm 8, 9, \mp 1), (\pm 2, 9, \mp 4), (\pm 4, 9, \mp 2).$$

§ 118. Perioden der reducirten Formen einer Determinante. — Wenn $F = (a, b, a_1)$ eine reducirte Form einer positiven nichtquadratischen Determinante D ist und wir das in § 115 dargelegte Verfahren auf sie anwenden, so erhalten wir eine Reihe von Formen

$$(1) \qquad F, F_1, F_2, \ldots,$$

von denen jede der folgenden nach links benachbart ist, und die nach Satz V des § 116 sämmtlich reducirt sind. Nun ist aber die Anzahl aller reducirten Formen von D eine endliche; daher muss in der Reihe (1) einmal eine Form F_{m+n} erscheinen, welche mit einer schon vorausgegangenen Form F_m identisch ist. Dann werden aber auch die diesen beiden vorhergehenden Formen, nämlich F_{m+n-1} und F_{m-1} identisch sein müssen, da sie derselben Form nach links benachbart sind. Aus demselben Grunde sind weiter F_{m+n-2} und F_{m-2}, ebenso F_{m+n-3} und F_{m-3}, u. s. w., endlich auch F_n und F identisch. Es wird also die Anfangsform F in der Reihe (1) wiederholt erscheinen. Bezeichnet nun n die kleinste Zahl, für welche F_n mit F identisch ist, so lässt sich zeigen, dass die Formen

$$(2) \qquad F, F_1, F_2, \ldots, F_{n-1}$$

sämmtlich von einander verschieden sind. Wäre nämlich F_k identisch mit $F_{k+k'}$, wo sowohl k, als auch $k + k' < n$ vorausgesetzt wird und daher auch $k' < n$ ist, so würde $F_{k'}$ mit F identisch sein müssen, was der Annahme, dass n die kleinste Zahl sei, für welche diese Identität besteht, widerspricht. Die Formen der Reihe (2) sind also wirklich von einander verschieden und setzen, in unveränderter Reihenfolge beliebig oft wiederholt, die Reihe (1) zusammen, da

$$F_n,\ F_{2n},\ \ldots,\ F_{\lambda n} \text{ identisch mit } F,$$
$$F_{n+1},\ F_{2n+1},\ \ldots,\ F_{\lambda n+1} \text{ ,, } \quad \text{ ,, } F_1,$$

allgemein $F_{kn+k'}$ identisch mit $F_{k'}$ ist. Aus diesem Grunde nennt man die Formen (2) die Periode der Form F.

Man kann, von F ausgehend, auch die Formenreihe

(3) $$\ldots, F_{-k}, F_{-(k-1)}, \ldots, F_{-3}, F_{-2}, F_{-1}, F$$

bilden, von denen jede der folgenden nach rechts benachbart ist, und als Periode von F die Reihe

(4) $$F_{-(n-1)}, F_{-(n-2)}, \ldots, F_{-1}, F$$

nehmen. Auch erkennt man sofort, dass F_{-k} identisch mit F_{n-k} ist.

Beispiel. Für die Determinante 89 ist (8, 3, — 10) eine reducirte Form, deren Periode aus folgenden 14 Formen besteht:

(8, 3, — 10), (— 10, 7, 4), (4, 9, — 2), (— 2, 9, 4),
(4, 7, — 10), (— 10, 3, 8), (8, 5, — 8), (— 8, 3, 10),
(10, 7, — 4), (— 4, 9, 2), (2, 9, — 4), (— 4, 7, 10),
(10, 3, — 8), (— 8, 5, 8).

Lehrsatz I. Die Periode jeder reducirten Form enthält eine gerade Anzahl Glieder.

Beweis. Da die ersten Coefficienten der Formen F, F_1, F_2, ... abwechselnd die Vorzeichen + und — haben, so haben die ersten Coefficienten von $F, F_2, F_4, \ldots, F_{2k}$ dasselbe Vorzeichen. Wenn also F_n mit F identisch sein soll, so muss n eine gerade Zahl sein.

Lehrsatz II. Ist G eine reducirte Form der Determinante D, welche der Periode der reducirten Form F nicht angehört, so kann auch keine Form der Periode von G sich in der Periode von F vorfinden.

Beweis. Wäre G_k identisch mit F_i, so müsste G_{k+1} identisch mit F_{i+1}, allgemein $G_{k+m-k} = G_m$ identisch mit F_{i+m-k} sein, oder, wenn m die Anzahl der Formen bezeichnet, welche die Periode von G enthält, in welchem Falle G_m identisch mit G ist, es müsste sich G in der Periode von F vorfinden, was der Voraussetzung widerspricht.

Wenn also die Periode von F nicht alle reducirten Formen der Determinante D enthält, so können wir eine dieser Periode nicht angehörende Form G wählen und die

Periode von G bilden; diese enthält gleichfalls eine gerade Anzahl von Formen, die von denen der Periode von F verschieden sind. Sind jetzt die reducirten Formen der Determinante D noch nicht erschöpft, so wählen wir eine Form H, welche sich weder in der ersten, noch in der zweiten Periode vorfindet, und erhalten eine dritte Periode. So fahren wir fort, bis alle reducirten Formen von D untergebracht sind. Die reducirten Formen einer positiven nichtquadratischen Determinante lassen sich also in Perioden vertheilen, von denen jede eine gerade Anzahl Formen enthält, und zwar wird jede reducirte Form nur in einer dieser Perioden vorkommen.

Beispiele. I. Für die Determinante 19 giebt es zwei Perioden reducirter Formen, nämlich

$$(3, 2, -5), (-5, 3, 2), (2, 3, -5), (-5, 2, 3),$$
$$(3, 4, -1), (-1, 4, 3)$$

und

$$(5, 2, -3), (-3, 4, 1), (1, 4, -3), (-3, 2, 5),$$
$$(5, 3, -2), (-2, 3, 5).$$

II. $D = 50$.

1. Periode. $(7, 1, -7)$, $(-7, 6, 2)$, $(2, 6, -7)$, $(-7, 1, 7)$, $(7, 6, -2)$, $(-2, 6, 7)$.

2. Periode. $(5, 5, -5)$, $(-5, 5, 5)$.

3. Periode. $(1, 7, -1)$, $(-1, 7, 1)$.

III. $D = 95$.

1. Periode. $(5, 5, -14)$, $(-14, 9, 1)$, $(1, 9, -14)$, $(-14, 5, 5)$.

2. Periode. $(14, 5, -5)$, $(-5, 5, 14)$, $(14, 9, -1)$, $(-1, 9, 14)$.

3. Periode. $(7, 5, -10)$, $(-10, 5, 7)$, $(7, 9, -2)$, $(-2, 9, 7)$.

4. Periode. $(10, 5, -7)$, $(-7, 9, 2)$, $(2, 9, -7)$, $(-7, 5, 10)$.

§ 119. Gefährten von reducirten Formen und von Perioden. — Eine reducirte Form heisst der Gefährte

einer andern, wenn beide aus denselben, aber in umgekehrter Reihenfolge geschriebenen Gliedern bestehen. So ist $(3, 8, -5)$ der Gefährte von $(-5, 8, 3)$, $(\pm a, b, \mp a_1)$ der Gefährte von $(\mp a_1, b, \pm a)$.

Lehrsatz I. Sind F und f zwei reducirte Formen einer Determinante D, und ist F der Gefährte von f, so enthält die Periode von F genau so viele Formen wie die von f, und zwar ist jede Form von f der Gefährte einer Form von F.

Beweis. Wir bilden die Form F_{-1}, welche F nach links benachbart ist, und die Form f_1, welche f nach rechts benachbart ist. Dann erkennen wir aus der Bildungsweise dieser Formen F_{-1}, f_1 sofort, dass beide Gefährten sein werden. Daraus folgt weiter, dass auch F_{-2} und f_2, allgemein F_{-k} und f_k Gefährten sind. Ist nun

$$F_{-m}, F_{-(m-1)}, \ldots, F_{-2}, F_{-1}, F$$

die Periode von F und

$$f, f_1, f_2, \ldots, f_{n-1}$$

diejenige von f, so muss $m = n - 1$ sein.

Wäre nämlich $m < n - 1$, so würde die links von F_{-m} stehende Form, d. i. F, der Gefährte von f_{m+1} sein. Nach der Voraussetzung ist aber f der Gefährte von F; also müsste die Form f mit einem Gliede f_{m+1} ihrer Periode identisch sein.

Ebenso würde die Annahme $m > n - 1$ zu dem Ergebnisse führen, dass die Form F mit einem Gliede ihrer Periode identisch wäre.

Da beides unmöglich ist, so muss $m = n - 1$ sein, d. h. beide Perioden enthalten gleich viel Glieder.

Von zwei Perioden von solcher Beschaffenheit, dass die Formen der einen beziehungsweise die Gefährten der Formen der andern sind, sagt man, die eine Periode sei der Gefährte der andern.

Beispiel. Für die Determinante 82 giebt es 4 Perioden reducirter Formen:

1. Periode. $(9, 1, -9)$, $(-9, 8, 2)$, $(2, 8, -9)$,
$(-9, 1, 9)$, $(9, 8, -2)$, $(-2, 8, 9)$.

2. Periode. (6, 4, — 11), (— 11, 7, 3), (3, 8, — 6), (— 6, 4, 11), (11, 7, — 3), (— 3, 8, 6).

3. Periode. (— 11, 4, 6), (6, 8, — 3), (— 3, 7, 11), (11, 4, — 6), (— 6, 8, 3), (3, 7, — 11).

4. Periode. (1, 9, — 1), (— 1, 9, 1).

Die 2[te] und 3[te] Periode sind Gefährten.

Es kann auch vorkommen, dass eine Form und ihr Gefährte sich in derselben Periode vorfinden; dann ist die Periode ihr eigener Gefährte. Solcher Art sind im obigen Beispiel die 1[te] und die 4[te] Periode. In diesem Falle besteht der

Lehrsatz II. **Eine Periode, die ihr eigener Gefährte ist, enthält zwei ambige Formen.**

Beweis. Es sei

$$F,\ F_1,\ F_2,\ \ldots,\ F_{2n-1}$$

die Periode von F und F_k der Gefährte von F. Da F und F_k als Gefährten Zahlen mit entgegengesetzten Zeichen zu ersten Coefficienten haben, so muss k eine ungerade Zahl sein, die wir $2m+1$ nennen wollen. Es sind also F_{2m+1} und F, folglich auch F_{2m} und F_1, ebenso F_{2m-1} und F_2, u. s. w., endlich F_{m+1} und F_m Gefährten.

Es sei jetzt

$$F_m = (a_m, b_m, -a_{m+1})$$

und

$$F_{m+1} = (-a_{m+1}, b_{m+1}, a_{m+2}),$$

so geht aus der Bildungsweise der Periode hervor, dass

$$b_m + b_{m+1} \equiv 0 \ (\text{mod. } a_{m+1})$$

ist; da aber $b_m = b_{m+1}$ ist, so erhalten wir hieraus

$$2b_{m+1} \equiv 0 \ (\text{mod. } a_{m+1}),$$

und somit ist F_{m+1} eine ambige Form.

Dass die Periode von F noch eine zweite ambige Form enthält, beweist man auf folgende Weise: Da F mit F_{2n} identisch ist, so sind auch F_{2m+1} und F_{2n} Gefährten; folglich sind auch F_{2m+2} und F_{2n-1}, ebenso F_{2m+3} und F_{2n-2}, u. s. w., endlich F_{m+n+1} und F_{m+n} Gefährten. Hieraus folgt aber, wie oben, dass F_{m+n+1} eine ambige Form ist, und da $m+1$ und

$m + n + 1$ für den Modul $2n$ nicht congruent sind, so sind die beiden ambigen Formen, die wir erhalten haben, von einander verschieden.

Beispiel. Die erste Periode der reducirten Formen für die Determinante 82 hat die beiden ambigen Formen $(2, 8, -9)$, $(-2, 8, 9)$; die 4[te] Periode besteht aus zwei ambigen Formen.

Lehrsatz III. Jede Periode, die eine ambige Form enthält, ist ihr eigener Gefährte.

Beweis. Ist F_m eine ambige Form, so ist F_{m-1} der Gefährte von F_m, also die Periode ihr eigener Gefährte.

Zusatz. Eine Periode kann niemals nur eine ambige Form enthalten.

Lehrsatz IV. Eine Periode reducirter Formen kann nicht mehr als zwei ambige Formen enthalten.

Beweis. Wir nehmen an, die Periode

$$F, F_1, F_2, \ldots, F_{2n-1}$$

enthalte die drei ambigen Formen F_λ, F_μ, F_ν, wo λ, μ, ν ungleiche Zahlen seien, die zwischen 0 und $2n - 1$ liegen. Dann sind zunächst $F_{\lambda-1}$ und F_λ, ebenso $F_{\lambda-2}$ und $F_{\lambda+1}$, u. s. w., endlich F und $F_{2\lambda-1}$ Gefährten. Auf dieselbe Weise erkennt man, dass F und $F_{2\mu-1}$, sowie F und $F_{2\nu-1}$ Gefährten sein müssen. Es müssten also die drei Formen

$$F_{2\lambda-1}, F_{2\mu-1}, F_{2\nu-1}$$

identisch, somit die Zahlen $2\lambda - 1$, $2\mu - 1$, $2\nu - 1$ in Beziehung auf den Modul $2n$ und daher die Zahlen λ, μ, ν in Beziehung auf den Modul n congruent sein. Zwischen Null und $2n - 1$ liegen aber keine drei Zahlen, die für n als Modul congruent sind; folglich kann die Periode auch nicht drei oder mehr ambige Formen enthalten.

§ 120. Transformation einer reducirten Form in eine beliebige andere Form derselben Periode. — Es sei $f = (a, b, -a_1)$ eine reducirte Form der positiven nichtquadratischen Determinante D, und es seien auf die oben dargelegte Weise die beiderseits benachbarten reducirten Formen, also die nach beiden Seiten unbegrenzte Reihe

$$\ldots, (a_{-2}, b_{-2}, -a_{-1}), (-a_{-1}, b_{-1}, a), (a, b, -a_1),$$
$$(-a_1, b_1, a_2), \ldots$$

gebildet, deren Glieder beziehungsweise mit

$$\ldots, f_{-2}, f_{-1}, f, f_1, \ldots$$

bezeichnet werden sollen. Wir stellen uns die Aufgabe, eine eigentliche Substitution zu suchen, welche irgend ein Glied der Reihe in irgend ein anderes transformire.

Setzen wir, wie im Falle einer negativen Determinante,

$$(1) \quad \ldots, \frac{b_{-2}+b_{-1}}{-a_{-1}} = h_{-1}, \quad \frac{b_{-1}+b}{a} = h_0, \quad \frac{b+b_1}{-a_1} = h_1, \ldots$$

und nehmen an, f gehe in f_k über durch die Substitution

$$\begin{cases} x = \alpha_k x_k + \beta_k y_k \\ y = \gamma_k x_k + \delta_k y_k, \end{cases}$$

so ergiebt sich wie früher, dass

$$(2) \qquad \begin{cases} \alpha_k = \beta_{k-1}, \ \beta_k = h_k \beta_{k-1} - \beta_{k-2}, \\ \gamma_k = \delta_{k-1}, \ \delta_k = h_k \delta_{k-1} - \delta_{k-2} \end{cases}$$

ist, und da wir die Werthe

$$\alpha_1 = 0, \ \beta_1 = -1, \ \gamma_1 = 1, \ \delta_1 = h_1$$

kennen, so ist die Aufgabe für positive Werthe von k (für die von f aus nach rechts liegenden Glieder der Reihe) erledigt.

Weiter wird nach § 98 f in f_{-1} transformirt durch die Substitution

$$x = h x_{-1} + y_{-1}, \ y = -x_{-1},$$

allgemein $f_{-(k-1)}$ in f_{-k} durch

$$(3) \qquad x_{-(k-1)} = h_{-(k-1)} x_{-k} + y_{-k}, \ y_{-(k-1)} = -x_{-k}.$$

Nehmen wir nun an, f gehe in f_{-k} über durch die Substitution

$$\begin{cases} x = \alpha_{-k} x_{-k} + \beta_{-k} y_{-k} \\ y = \gamma_{-k} x_{-k} + \delta_{-k} y_{-k}, \end{cases}$$

so verwandelt sich f in $f_{-(k-1)}$, wenn man

$$\begin{cases} x = \alpha_{-(k-1)} x_{-(k-1)} + \beta_{-(k-1)} y_{-(k-1)} \\ y = \gamma_{-(k-1)} x_{-(k-1)} + \delta_{-(k-1)} y_{-(k-1)} \end{cases}$$

setzt, und $f_{-(k-1)}$ in f_{-k} durch die Substitution (3), also f in f_{-k}, wenn

$$\begin{cases} x = \alpha_{-(k-1)} (h_{-(k-1)} x_{-k} + y_{-k}) - \beta_{-(k-1)} x_{-k} \\ y = \gamma_{-(k-1)} (h_{-(k-1)} x_{-k} + y_{-k}) - \delta_{-(k-1)} x_{-k} \end{cases}$$

gesetzt wird. Es muss somit

$$\begin{cases} \alpha_{-k} = h_{-(k-1)}\alpha_{-(k-1)} - \beta_{-(k-1)} \\ \beta_{-k} = \alpha_{-(k-1)} \\ \gamma_{-k} = h_{-(k-1)}\gamma_{-(k-1)} - \delta_{-(k-1)} \\ \delta_{-k} = \gamma_{-(k-1)} \end{cases}$$

sein. Die Werthe von α_{-k}, γ_{-k} lassen sich offenbar auch folgendermassen schreiben:

$$(4) \qquad \begin{cases} \alpha_{-k} = h_{-(k-1)}\alpha_{-(k-1)} - \alpha_{-(k-2)} \\ \gamma_{-k} = h_{-(k-1)}\gamma_{-(k-1)} - \gamma_{-(k-2)}\,, \end{cases}$$

und da, wie wir gesehen haben,

$$\alpha_{-1} = h\,,\ \beta_{-1} = 1\,,\ \gamma_{-1} = -1\,,\ \delta_{-1} = 0$$

ist, so ist die Aufgabe auch für negative k (für die links von f liegenden Glieder der Reihe) erledigt.

Durch Einschaltung der Substitution, welche die Coefficienten

$$\alpha_0 = 1\,,\ \beta_0 = 0\,,\ \gamma_0 = 0\,,\ \delta_0 = 1$$

hat, und welche f offenbar unverändert lässt, bewirken wir, dass die gleichnamigen Coefficienten aller Substitutionen nach beiden Seiten hin unbegrenzte Reihen bilden, welche beziehungsweise den Gesetzen gehorchen

$$(5) \qquad \begin{cases} \alpha_{m+1} = h_m\alpha_m - \alpha_{m-1} \\ \beta_{m+1} = h_{m+1}\beta_m - \beta_{m-1} \\ \gamma_{m+1} = h_m\gamma_m - \gamma_{m-1} \\ \delta_{m+1} = h_{m+1}\delta_m - \delta_{m-1}\,, \end{cases}$$

wo m jede positive oder negative ganze Zahl sein kann.

Beispiele. I. Es soll die dritte Form der oben für $D = 82$ erhaltenen dritten Periode in die übrigen transformirt werden. Es ist

$$(-11,\ 4,\ 6) = f_{-2},\ (6,\ 8,\ -3) = f_{-1},\ (-3,\ 7,\ 11) = f,$$
$$(11,\ 4,\ -6) = f_1,\ (-6,\ 8,\ 3) = f_2,\ (3,\ 7,\ -11) = f_3,$$

also

$$h_{-1} = 2\,,\ h_0 = -5\,,\ h_1 = 1\,,\ h_2 = -2\,,\ h_3 = 5\,.$$

Wir schreiben nun die Werthe h in eine Horizontallinie und unter h_0 die Zahl $\alpha_0 = 1$, unter h_1 ebenso $\beta_0 = 0$. Darauf multipliciren wir h_1 mit β_0, subtrahiren vom Produkt α_0 und

schreiben den Rest unter h_2. So fortfahrend finden wir $\beta_2 = 2$, $\beta_3 = 11$. Nach demselben Gesetz führen wir die Reihe rückwärts und erhalten $\beta_{-2} = -5$; der letzteren Zahl würde (nach diesem Gesetz) -11 vorhergehen. Ebenso bilden wir eine zweite Reihe, indem wir $\gamma_0 = 0$ unter h_0 und $\delta_0 = 1$ unter h_1 setzen und wie oben verfahren. Es ist dann allgemein die erste unter h_k stehende Zahl β_{k-1}, die links davon stehende Zahl α_{k-1}, die zweite unter h_k stehende Zahl δ_{k-1} und die links davon stehende Zahl γ_{k-1}. Die Anordnung für dieses Beispiel würde also folgende sein:

	$h_{-1}=2$	$h_0=-5$	$h_1=1$	$h_2=-2$	$h_3=5$	
-11	-5	1	0	-1	2	11
-2	-1	0	1	1	-3	-16

II. Die Determinante 103 hat 2 Perioden reducirter Formen; die eine ist

$f_{-4} = (9, 2, -11)$, $f_{-3} = (-11, 9, 2)$, $f_{-2} = (2, 9, -11)$, $f_{-1} = (-11, 2, 9)$, $f = (9, 7, -6)$, $f_1 = (-6, 5, 13)$, $f_2 = (13, 8, -3)$, $f_3 = (-3, 10, 1)$, $f_4 = (1, 10, -3)$, $f_5 = (-3, 8, 13)$, $f_6 = (13, 5, -6)$, $f_7 = (-6, 7, 9)$.

Es soll f in alle übrigen Formen transformirt werden. Man erhält die Tabelle

	$h_{-3}=-1$	$h_{-2}=9$	$h_{-1}=-1$	$h_0=1$
21	-19	-2	1	1
-11	10	1	-1	0

$h_1=-2$	$h_2=1$	$h_3=-6$	$h_4=20$	$h_5=-6$
0	-1	-1	7	141
1	-2	-3	20	403

$h_6=1$	$h_7=-2$	
-853	-994	2841
-2438	-2841	8120

Danach geht z. B. f in f_4 über durch die Substitution

$$\begin{cases} x = 7x' + 141y' \\ y = 20x' + 403y', \end{cases}$$

u. s. w.

§ 121. Zusammenhang zwischen der Form (a, b, c) und den Wurzeln der Gleichung $a + 2b\omega + c\omega^2 = 0$. — Wir haben oben gesehen, dass die für jede Determinante vorhandenen reducirten Formen sich in Perioden ordnen lassen, und dass sämmtliche Formen einer jeden Periode unter einander eigentlich äquivalent sind. Es fragt sich nun, ob nicht auch zwei reducirte Formen, die verschiedenen Perioden angehören, äquivalent sein können. Diese schwierige Frage wollen wir nach Lejeune Dirichlet (Abhandlungen der Berliner Akademie, 1854) behandeln, dessen Betrachtungsweise nicht allein die Sache erheblich vereinfacht, sondern auch den an sich interessanten Zusammenhang zwischen den Gliedern der Periode einer reducirten Form und der Kettenbruch-Entwicklung der irrationalen Wurzeln einer von den Coefficienten der Anfangsform abhängigen Gleichung zweiten Grades ins Licht treten lässt.

Wir denken uns die Form

$$ax^2 + 2bxy + cy^2 = (a, b, c)$$

gleich Null gesetzt, also die Gleichung

$$a + 2b\omega + c\omega^2 = 0$$

gebildet, deren Unbekannte ω das Verhältniss $\frac{y}{x}$ ausdrückt, und welche die Wurzeln

$$\omega = \frac{-b \mp \sqrt{D}}{c}$$

hat. Darin ist $D = b^2 - ac$ (die Determinante der Form), und wir setzen fest, dass unter $\sqrt{D}$ immer die positive Quadratwurzel aus D verstanden werden soll. Die dem oberen Zeichen entsprechende Wurzel soll die erste, die dem unteren Zeichen entsprechende die zweite Wurzel der Form (a, b, c) heissen.

Liegt eine zweite Form

$$a_1 x_1^2 + 2b_1 x_1 y_1 + c_1 y_1^2$$

vor, so besitzt auch diese in dem dargelegten Sinne zwei Wurzeln

$$\omega_1 = \frac{-b_1 \mp \sqrt{D_1}}{c_1},$$

und wir werden zwei Wurzeln zweier Formen gleichnamig nennen, wenn beide erste oder beide zweite Wurzeln sind; im entgegengesetzten Falle sollen dieselben ungleichnamig heissen.

Wie eine Form ihre beiden Wurzeln bestimmt, so wird umgekehrt offenbar auch eine Form bestimmt sein, sobald ihre Wurzeln gegeben sind. Ist z. B. $\frac{3 \mp \sqrt{19}}{5}$ der Ausdruck für die Wurzeln einer Form, so ist der dritte Coefficient der Form 5, der zweite -3, und damit die Determinante $+19$ sei, muss man den ersten Coefficienten $= -2$ setzen; die Form ist also $(-2, -3, 5)$.

Anmerkung. Für eine reducirte Form $(a, b, -a_1)$ ergiebt sich Folgendes:

Die erste Wurzel $\frac{b + \sqrt{D}}{a_1}$ dieser Form ist offenbar positiv und > 1; denn nach § 115 ist $[a_1] < b + \sqrt{D}$. Die zweite Wurzel $\frac{b - \sqrt{D}}{a_1}$ dagegen ist negativ ($\sqrt{D} > b$), und da

$$[a_1] > \sqrt{D} - b$$

ist, so ist ihr absoluter Werth < 1.

Es seien jetzt

$f = ax^2 + 2bxy + cy^2$ und $f_1 = a_1 x_1^2 + 2b_1 x_1 y_1 + c_1 y_1^2$

zwei eigentlich äquivalente Formen, und zwar möge f in f_1 durch die Substitution

$$(1) \qquad \begin{cases} x = \alpha x_1 + \beta y_1 \\ y = \gamma x_1 + \delta y_1 \end{cases}$$

übergehen, wo

$$(2) \qquad \alpha\delta - \beta\gamma = +1$$

ist. Dann gelten folgende Sätze:

Lehrsatz I. Bezeichnen ω und ω_1 zwei gleichnamige Wurzeln der beiden Formen f, f_1, so bestehen die beiden Gleichungen

$$(3) \qquad \omega = \frac{\gamma + \delta\omega_1}{\alpha + \beta\omega_1} \quad \text{und} \quad \omega_1 = \frac{\gamma - \alpha\omega}{\beta\omega - \delta}.$$

Beweis. Es ist

$$\omega = \frac{y}{x} = \frac{\gamma x_1 + \delta y_1}{\alpha x_1 + \beta y_1} = \frac{\gamma + \delta \frac{y_1}{x_1}}{\alpha + \beta \frac{y_1}{x_1}} = \frac{\gamma + \delta \omega_1}{\alpha + \beta \omega_1}.$$

Da umgekehrt die zweite Form in die erste transformirt wird, wenn man

$$\begin{cases} x_1 = \delta x - \beta y \\ y_1 = -\gamma x + \alpha y \end{cases}$$

setzt, so ist

$$\omega_1 = \frac{y_1}{x_1} = \frac{-\gamma x + \alpha y}{\delta x - \beta y} = \frac{-\gamma + \alpha \omega}{\delta - \beta \omega}.$$

Zusatz. Zwischen gleichnamigen Wurzeln zweier benachbarten reducirten Formen bestehen die Gleichungen

$$(4) \qquad \omega = -h - \frac{1}{\omega_1} \quad \text{und} \quad \omega_1 = -\frac{1}{\omega + h}.$$

Beweis. In diesem Falle ist nach § 120

$$\alpha = 0, \ \beta = -1, \ \gamma = +1, \ \delta = h,$$

und durch Einsetzung dieser Werthe in (3) erhält man sofort die Gleichungen (4).

Lehrsatz II. Findet für ein Paar gleichnamiger Wurzeln der Formen f, f_1 der Determinante D eine der Gleichungen (3) statt, und erfüllen zugleich die ganzen Zahlen α, β, γ, δ die Bedingung (2), so sind die Formen äquivalent, und die erste geht durch die Substitution (1) in die zweite über.

Beweis. Es ist

$$\omega = \frac{-b + \sqrt{D}}{c}, \qquad \omega_1 = \frac{-b_1 + \sqrt{D}}{c_1}.$$

Nun soll

$$\frac{-b_1 + \sqrt{D}}{c_1} = \frac{\gamma - \alpha\left(\frac{-b + \sqrt{D}}{c}\right)}{\beta\left(\frac{-b + \sqrt{D}}{c}\right) - \delta} = \frac{\gamma c + \alpha b - \alpha\sqrt{D}}{-\beta b - \delta c + \beta\sqrt{D}}$$

sein. Wir erweitern die rechte Seite, um den Nenner rational zu machen, mit $\beta b + \delta c + \beta\sqrt{D}$ und erhalten

$$\frac{-b_1 + \sqrt{D}}{c_1} = \frac{c\{a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta\} - (\alpha\delta - \beta\gamma)c\sqrt{D}}{-c(a\beta^2 + 2b\beta\delta + c\delta^2)}$$

$$= \frac{-\{a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta\} + \sqrt{D}}{a\beta^2 + 2b\beta\delta + c\delta^2}.$$

Somit [§ 98] ist (a_1, b_1, c_1) wirklich die Form, in welche (a, b, c) durch die Substitution (1) transformirt wird.

Der Beweis würde sich ebenso gestaltet haben, wenn wir von den beiden ersten Wurzeln der Formen ausgegangen wären.

§ 122. Zusammenhang zwischen den Gliedern der Periode einer reducirten Form und der Kettenbruch-Entwicklung einer Wurzel der Ausgangsform. —

Es sei

$$\ldots, (+a_{-2}, b_{-2}, -a_{-1}), \quad (-a_{-1}, b_{-1}, +a),$$
$$(+a, b, -a_1), \quad (-a_1, b_1, a_2), \ldots$$

oder

$$f_{-2}, \quad f_{-1}, \quad f_0, \quad f_1, \ldots$$

die beiderseits unbegrenzte Reihe reducirter Formen, von denen jede der folgenden nach links benachbart ist. Ferner sei wieder

$$\ldots, \quad \frac{b_{-2} + b_{-1}}{-a_{-1}} = h_{-1}, \quad \frac{b_{-1} + b}{+a} = h_0, \quad \frac{b + b_1}{-a_1} = h_1, \ldots$$

Da es gleichgiltig ist, welchem Gliede der Reihe wir den Index Null beilegen, d. h. welches Glied wir als Anfangsglied ansehen, so soll zur Vermeidung unnützer Unterscheidungen angenommen werden, dass der erste Coefficient der Form f_0, also überhaupt der erste Coefficient jeder Form mit geradem Index positiv sei. Unter dieser Voraussetzung werden auch $h_0, h_2, h_4, \ldots$ positiv sein, jedes h mit ungeradem Index dagegen negativ. Ebenso erkennt man leicht aus dem Ausdruck der Wurzeln, dass die erste Wurzel jeder Form positiv oder negativ ist, je nachdem die Form einen geraden oder ungeraden Index hat. Mit den zweiten Wurzeln verhält es sich umgekehrt.

Sind nun $\omega_0, \omega_1, \omega_2, \ldots$ gleichnamige (etwa erste) Wurzeln der Formen $f_0, f_1, f_2, \ldots$, so ist nach dem Zusatz zum Lehrsatz I des vorigen Paragraphen

$$\omega_0 = -h_1 - \frac{1}{\omega_1}, \quad \omega_1 = -h_2 - \frac{1}{\omega_2},$$
$$\omega_2 = -h_3 - \frac{1}{\omega_3}, \dots.$$

Multipliciren wir jetzt die zweite, vierte, u. s. w. dieser Gleichungen mit -1, so erhalten wir das System

$$\omega_0 = -h_1 + \frac{1}{-\omega_1}, \quad -\omega_1 = h_2 + \frac{1}{\omega_2},$$
$$\omega_2 = -h_3 + \frac{1}{-\omega_3}, \quad -\omega_3 = h_4 + \frac{1}{\omega_4},$$
$$\dots\dots\dots\dots\dots\dots$$

Da $h_1, h_3, \dots$ negativ sind, so sind $-h_1, -h_3, \dots$ positive Zahlen. Wir wollen für diese positiven Zahlen der Kürze halber einfach $h_1, h_3, \dots$ schreiben. Dann sehen wir Folgendes: Die erste Wurzel ω_0 der Ausgangsform ist gleich dem unendlichen Kettenbruch, dessen unvollständige Quotienten die absoluten Werthe der oben definirten Grössen h sind. Da letztere eine rein periodische Reihe bilden, so ist auch der Kettenbruch rein periodisch.

Beispiele. I. Die Determinante 29 hat 2 Perioden reducirter Formen:

1. Periode.

(5, 2, — 5), (— 5, 3, 4), (4, 5, — 1), (— 1, 5, 4),
(4, 3, — 5), (— 5, 2, 5), (5, 3, — 4), (— 4, 5, 1),
(1, 5, — 4), (— 4, 3, 5).

Die erste Wurzel der Gleichung

$$5 + 4\omega - 5\omega^2 = 0$$

ist

$$\omega = \frac{2 + \sqrt{29}}{5}.$$

Da nun

$$h_1 = -1, \quad h_2 = 2, \quad h_3 = -10, \quad h_4 = 2,$$
$$h_5 = -1, \quad h_6 = 1, \quad h_7 = -2, \quad h_8 = 10,$$
$$h_9 = -2, \quad h_{10} = 1$$

ist, so ist ω gleich dem rein periodischen Kettenbruch, für welchen

1, 2, 10, 2, 1, 1, 2, 10, 2, 1

die Periode der unvollständigen Quotienten ist.

[Man beachte den Umstand, dass diese Periode eine Doppelperiode ist].

2. Periode. $(2, 5, -2)$, $(-2, 5, 2)$.

Die erste Wurzel der Gleichung $2 + 10\omega - 2\omega^2 = 0$ ist

$$\omega = \frac{5 + \sqrt{29}}{2}.$$

Nun ist

$$h_1 = -5, \quad h_2 = 5,$$

also

$$\frac{5 + \sqrt{29}}{2} = 5 + \cfrac{1}{5 + \cfrac{1}{5 + \cdots}}$$

II. Eine Periode von 91 ist

$(9, 1, -10)$, $(-10, 9, 1)$, $(1, 9, -10)$, $(-10, 1, 9)$,
$(9, 8, -3)$, $(-3, 7, 14)$, $(14, 7, -3)$, $(-3, 8, 9)$.

Die Gleichung $9 + 2\omega - 10\omega^2 = 0$ hat die erste Wurzel $\frac{+1 + \sqrt{91}}{10}$. Für diese ergiebt sich, da

$$h_1 = -1, \quad h_2 = 18, \quad h_3 = -1, \quad h_4 = 1,$$
$$h_5 = -5, \quad h_6 = 1, \quad h_7 = -5, \quad h_8 = 1$$

ist, der Kettenbruch, welcher zur Periode die unvollständigen Quotienten 1, 18, 1, 1, 5, 1, 5, 1 hat.

§ 123. Aequivalenz der Formen einer positiven nichtquadratischen Determinante. —

Hilfssatz. Finden zwischen zwei Grössen ω, ω_1 und den ganzen Zahlen α, β, γ, δ, deren erste nicht Null ist, die Relationen

$$\omega = \frac{\gamma + \delta\omega_1}{\alpha + \beta\omega_1}, \quad \alpha\delta - \beta\gamma = 1$$

statt, so lässt sich immer eine Gleichung der Form [§ 34.]

$$\omega = (\lambda, m, \ldots, r, \sigma, \omega_1)$$

bilden, in welcher von den ganzen Zahlen $\lambda, m, \ldots, r, \sigma$ nur die erste und die letzte Null oder negativ sein können, die Zwischenglieder aber, wenn sie nicht ganz fehlen, positiv und in gerader Anzahl vorhanden sind.

Beweis. Wir dürfen, ohne die Allgemeinheit der Betrachtung zu beeinträchtigen, α als positiv voraussetzen; denn wenn α negativ wäre, so dürften wir jeder der 4 Grössen α, β, γ, δ das entgegengesetzte Zeichen geben, ohne dass dadurch die Gleichungen, die unsere Voraussetzung bilden, geändert würden.

Ist nun $\alpha = 1$, so erhält man sofort $\delta = 1 + \beta\gamma$, also geht die Gleichung für ω über in

$$\omega = \frac{\gamma + (1 + \beta\gamma)\omega_1}{1 + \beta\omega_1} = \frac{\gamma(1 + \beta\omega_1) + \omega_1}{1 + \beta\omega_1} = \gamma + \cfrac{1}{\beta + \cfrac{1}{\omega_1}}.$$

Ist dagegen $\alpha > 1$, so verwandle man den rationalen Bruch $\frac{\gamma}{\alpha}$ in einen Kettenbruch, wobei alle Divisionsreste positiv gewählt werden mögen. Wir nehmen an, es ergebe sich

$$\frac{\gamma}{\alpha} = (\lambda, m, \ldots, r);$$

dann sind die unvollständigen Quotienten $m, \ldots, r$ positiv. Nur λ kann auch Null oder negativ sein. Ferner lässt es sich so einrichten, dass die Anzahl der Grössen $m, \ldots, r$ eine gerade ist, da wir im entgegengesetzten Falle r durch $r - 1 + \frac{1}{1}$ ersetzen, die Zahl der in Rede stehenden Quotienten also um eine Einheit vermehren könnten. Es sei $2k$ die Anzahl der Grössen $m, \ldots, r$. Ferner nehmen wir an, es seien die Näherungsbrüche gebildet, die sämmtlich irreducibel, und deren Nenner offenbar positive Zahlen sein werden. Der letzte Näherungsbruch ist $\frac{\gamma}{\alpha}$ selbst, der vorletzte $\frac{Z_{2k}}{N_{2k}}$; dann ist bekanntlich

$$\gamma N_{2k} - \alpha Z_{2k} = -1.$$

Es ist aber auch

$$\gamma\beta - \alpha\delta = -1,$$

also

$$\gamma(N_{2k} - \beta) = \alpha(Z_{2k} - \delta).$$

Da γ und α prim zu einander sind, so muss γ in $Z_{2k} - \delta$ und α ebenso oft in $N_{2k} - \beta$ aufgehen. Es sei

$$\frac{Z_{2k} - \delta}{\gamma} = \frac{N_{2k} - \beta}{\alpha} = -\sigma,$$

so ist $$\delta = \gamma\sigma + Z_{2k}, \quad \beta = \alpha\sigma + N_{2k}.$$

Folglich schliesst sich der Bruch $\frac{\delta}{\beta}$ der Reihe der Näherungsbrüche direkt an, wenn der Reihe der unvollständigen Quotienten der neue Quotient σ zugefügt wird, oder es ist

$$\frac{\delta}{\beta} = (\lambda, m, \ldots r, \sigma).$$

Fügt man endlich als letzten Quotienten die Grösse ω_1 an, so erhält man, wie aus der Zusammenstellung

λ	m	n	$\ldots$	r	σ	ω_1	
$\frac{1}{0}$	$\frac{\lambda}{1}$	$\frac{m\lambda + 1}{m}$	$\ldots$	$\frac{Z_{2k}}{N_{2k}}$	$\frac{\gamma}{\alpha}$	$\frac{\delta}{\beta}$	$\frac{\delta\omega_1 + \gamma}{\beta\omega_1 + \alpha}$

sofort erhellt, als letzten Näherungsbruch $\frac{\delta\omega_1 + \gamma}{\beta\omega_1 + \alpha}$, und da diese Grösse $= \omega$ ist, so ist in der That

$$\omega = (\lambda, m, \ldots, r, \sigma, \omega_1).$$

Aufgabe. Man hat eine irrationale Grösse ω in einen Kettenbruch

$$\omega = (\alpha, \beta, \ldots, \mu, \nu, p, q, r, \ldots, u, v, \ldots)$$

entwickelt, in welchem die Glieder erst von p incl. an positive ganze Zahlen sind, während einige der vorhergehenden unvollständigen Quotienten den Werth Null haben oder negativ sind. Man soll den Kettenbruch in einen andern verwandeln, welcher nur positive Glieder enthält.

Lösung. Wir werden sehen, dass sich die Aufgabe durch eine Reihe von Umformungen des Kettenbruchs lösen lässt, bei welchen die Glieder, die auf ein hinlänglich weit entferntes Glied u folgen, unberührt bleiben, während sich die Anzahl der von den Umformungen betroffenen Glieder um eine gerade oder ungerade Zahl ändert, je nachdem ω positiv oder negativ ist.

Dies zu zeigen, nehmen wir an, ν sei der letzte unvollständige Quotient, der nicht positiv ist. Zugleich setzen wir aber zunächst voraus, dass ν nicht der erste unvollständige Quotient überhaupt sei. Dann sind folgende Fälle zu unterscheiden:

1. **Fall.** Es sei $\nu = 0$. Dann ist der in Rede stehende Theil des Kettenbruchs

$$\mu + \cfrac{1}{0 + \cfrac{1}{p + \cdot_{\textstyle .}}} = (\mu + p) + \cdot_{\textstyle .}\,;$$

es ist also an die Stelle der drei Glieder μ, $\nu = 0$, p das eine Glied $\mu + p$ getreten, d. h. die Anzahl der Glieder hat sich um eine gerade Zahl verändert, während die in dem Vorhandensein negativer oder verschwindender unvollständiger Quotienten bestehende Unregelmässigkeit um wenigstens eine Stelle nach links gedrängt ist.

2. Fall. Es sei ν eine negative Zahl $-n$ und $n > 1$. Dann liefert die Identität

$$g + \frac{1}{-h} = (g-1) + \cfrac{1}{1 + \cfrac{1}{h-1}}$$

zunächst

$$g + \cfrac{1}{-h + \cfrac{1}{x}} = g + \cfrac{1}{-\left[h - \cfrac{1}{x}\right]} = (g-1) + \cfrac{1}{1 + \cfrac{1}{(h-1) - \cfrac{1}{x}}}.$$

Wenden wir dies auf den in Rede stehenden Theil des Kettenbruchs an, so erhalten wir

$$\mu + \cfrac{1}{-n + \cfrac{1}{p'}} = (\mu - 1) + \cfrac{1}{1 + \cfrac{1}{(n-1) - \cfrac{1}{p'}}};$$

darin bezeichnet p' den mit p beginnenden Theil des Kettenbruchs. Weiter liefert dieselbe Identität, wenn der mit q beginnende Theil des Kettenbruchs mit q' bezeichnet wird,

$$(n-1) - \frac{1}{p'},$$

d. i.

$$(n-1) + \cfrac{1}{-\left[p + \cfrac{1}{q'}\right]} = (n-2) + \cfrac{1}{1 + \cfrac{1}{(p-1) + \cfrac{1}{q'}}};$$

es ist also

$$\mu + \cfrac{1}{-n + \cfrac{1}{p + \cfrac{1}{q'}}} = (\mu - 1,\ 1,\ n - 2,\ 1,\ p - 1,\ q').$$

An die Stelle der drei geänderten unvollständigen Quotienten μ, ν, p sind also die fünf $\mu - 1$, 1, $n - 2$, 1, $p - 1$ getreten, von denen höchstens der erste, d. i. $\mu - 1$, negativ ist. Jede der Grössen $n - 2$, $p - 1$ kann gleich Null sein,

aber diese Unregelmässigkeit lässt sich auf die im 1. Fall angegebene Weise beseitigen. Jedenfalls ist die Unregelmässigkeit im Kettenbruch eine Stelle links geschoben, und dabei hat sich die Anzahl der unvollständigen Quotienten um eine gerade Zahl geändert.

3. Fall. Es sei $\nu = -1$ und zugleich $p > 1$.

Dann ist

$$\mu + \cfrac{1}{-1 + \cfrac{1}{p + \cfrac{1}{q}}} = (\mu - 2) + \cfrac{1}{1 + \cfrac{1}{(p-2) + \cfrac{1}{q}}}.$$

Wenn hierin $p - 2 = 0$ sein sollte, so würde das im 1. Fall dargelegte Verfahren diese Unregelmässigkeit leicht beseitigen, und da hierbei die Anzahl der unvollständigen Quotienten sich um eine gerade Zahl ändern würde, während die Beseitigung des negativen Gliedes $\nu = -1$ in diesem Falle jene Anzahl überhaupt unverändert lässt (die drei Glieder μ, -1, p werden durch $\mu - 2$, 1, $p - 2$ ersetzt), so kann auch hier jene Anzahl sich nur um eine gerade Zahl ändern.

4. Fall. Es sei $\nu = -1$ und zugleich $p = 1$. Dann besteht die Identität

$$\mu + \cfrac{1}{-1 + \cfrac{1}{1 + \cfrac{1}{q}}} = \mu - 1 - q,$$

also erhalten wir für den in Rede stehenden Theil des Kettenbruchs

$$\mu + \cfrac{1}{-1 + \cfrac{1}{1 + \cfrac{1}{q + \cfrac{1}{r}}}} = \mu - 1 - q - \frac{1}{r}$$

oder nach der im 2. Falle benutzten Identität

$$\mu - 2 - q + \cfrac{1}{1 + \cfrac{1}{r - 1 + \cfrac{1}{s}}}.$$

Sollte $r - 1 = 0$ sein, so würden wir wie im 1. Falle verfahren. Da die fünf unvollständigen Quotienten μ, -1, 1, q, r durch die drei $\mu - 2 - q$, 1, $r - 1$ ersetzt sind, so hat sich die Anzahl derselben um eine gerade Zahl geändert.

In allen Fällen haben wir also die Unregelmässigkeit im Kettenbruch um wenigstens eine Stelle nach links gedrängt,

und dabei hat sich die Anzahl der Glieder um eine gerade Zahl geändert.

Durch wiederholte Anwendung dieses Verfahrens können wir bewirken, dass alle unvollständigen Quotienten des Kettenbruchs, mit Ausnahme des ersten, ganze positive Zahlen sind; dabei sind die Glieder von einer bestimmten in endlicher Entfernung liegenden Stelle an unverändert geblieben, und die Anzahl der veränderten Glieder hat um eine gerade Zahl zu- oder abgenommen.

Ist nun zugleich das erste Glied α nicht negativ, so ist das Verfahren geschlossen und der Satz, wie wir ihn oben formulirt hatten, bewiesen. Hat dagegen das erste Glied den negativen Werth $-\alpha$, so ist, wenn $\beta > 1$ ist,

$$-\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma'}} = -\left[\alpha + \cfrac{1}{-\left(\beta + \cfrac{1}{\gamma'}\right)}\right]$$

$$= -\left[(\alpha - 1) + \cfrac{1}{1 + \cfrac{1}{(\beta - 1) + \cfrac{1}{\gamma'}}}\right],$$

und wenn $\beta = 1$ ist, so erhält man

$$-\alpha + \cfrac{1}{1 + \cfrac{1}{\gamma + \cfrac{1}{\delta'}}} = -\frac{\alpha\gamma\delta' + \alpha\delta' - \gamma\delta' + \alpha - 1}{\gamma\delta' + \delta' + 1}$$

$$= -\left[(\alpha - 1) + \cfrac{1}{\gamma + 1 + \cfrac{1}{\delta'}}\right].$$

Bei dieser letzten Operation sind also, wenn $\beta > 1$ ist, die beiden Glieder $-\alpha$, β, durch die drei $\alpha - 1$, 1, $\beta - 1$, und wenn $\beta = 1$ ist, die drei Glieder $-\alpha$, 1, γ durch die beiden $\alpha - 1$, $\gamma + 1$ ersetzt. Somit ist, wenn der Kettenbruch einen negativen Werth hat, die Anzahl der geänderten Glieder um eine ungerade Zahl vermehrt oder vermindert worden.

Diese Betrachtungen werden uns einen einfachen Beweis des folgenden wichtigen Satzes liefern:

Lehrsatz. *Wenn zwei reducirte Formen einer positiven nichtquadratischen Determinante eigentlich äquivalent sind, so ist die eine ein Glied der Periode der andern.*

Beweis. Wir können uns für jede der beiden vorgelegten

Formen die Periode gebildet denken. Da nun alle Formen einer Periode unter einander äquivalent sind, so werden die vorgelegten Formen hinsichtlich der Aequivalenz sich ganz so verhalten, wie eine beliebige Form der ersten und eine beliebige Form der zweiten Periode. Wir wählen nun zum Vergleich aus jeder Periode eine Form, deren erster Coefficient positiv ist; dann wird auch die erste Wurzel jeder dieser beiden Formen positiv sein. Die aus der ersten Periode genommene Form sei $\varphi_0 = (a, b, c)$, die zugehörige erste Wurzel ω_0; aus der zweiten Periode sei $\Phi_0 = (A, B, C)$ mit der ersten Wurzel Ω_0 genommen.

Wie wir gesehen haben, lässt sich dann sowohl ω_0, als auch Ω_0 durch einen periodischen Kettenbruch ausdrücken, dessen unvollständige Quotienten ganze positive Zahlen sind.

Es sei

$$\omega_0 = (k_0, k_1, k_2, \ldots),$$
$$\Omega_0 = (K_0, K_1, K_2, \ldots).$$

Setzen wir jetzt voraus, beide Formen seien eigentlich äquivalent, und die erste gehe in die zweite durch die Substitution

$$\begin{cases} x = \alpha X + \beta Y \\ y = \gamma X + \delta Y \end{cases}$$

über, wo $\alpha\delta - \beta\gamma = +1$ ist, so besteht nach § 121 zwischen ω_0 und Ω_0 die Beziehung

$$\omega_0 = \frac{\gamma + \delta\Omega_0}{\alpha + \beta\Omega_0}.$$

Nun muss α von Null verschieden sein. Wäre nämlich $\alpha = 0$, so würde $\gamma = \pm 1$ sein, und die bekannte Transformationsgleichung

$$A = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$$

würde $A = c$ liefern, was unmöglich ist, da nach unserer Voraussetzung A eine positive, c eine negative Zahl ist.

Wenn aber α von Null verschieden ist, so liefert der obige Hilfssatz uns eine Gleichung von der Form

$$\begin{aligned} \omega_0 &= (\lambda, m, \ldots, r, \sigma, \Omega_0) \\ &= (\lambda, m, \ldots, r, \sigma, K_0, K_1, \ldots, K_r, \ldots), \end{aligned}$$

wo die Zahl der Glieder $\lambda, m, \ldots, r, \sigma$ eine gerade ist. Diese

Zahl sei $2g$. Werden aus dem Kettenbruch die Glieder, welche Null oder negativ sind, entfernt, so bleiben die Glieder von einer bestimmten Stelle an unverändert. Das erste Glied, welches unberührt bleibt, sei K_ν. Die Anzahl der vorhergehenden Glieder ändert sich, da ω_0 positiv ist, um eine gerade Zahl $2h$, und zwar ist h positiv, Null oder negativ, je nachdem die Anzahl dieser Glieder zunimmt, unverändert bleibt oder abnimmt. Nach der Umformung muss der Kettenbruch, da ω_0 sich nur auf eine Weise in einen Kettenbruch mit positiven Gliedern verwandeln lässt, mit dem oben für ω_0 gegebenen zusammenfallen. Es ist daher, wenn der Index ν eine gewisse Grenze überschreitet,

$$K_\nu = k_{2g+2h+\nu},$$

d. h. die Zahlen

$$K_\nu,\ K_{\nu+1},\ K_{\nu+2},\ \ldots,\ K_{\nu+\lambda},\ \ldots$$

sind beziehungsweise mit

$$k_{2g+2h+\nu},\ k_{2g+2h+\nu+1},\ k_{2g+2h+\nu+2},\ \ldots,\ k_{2g+2h+\nu+\lambda},\ \ldots$$

identisch. Ist nun $\nu + \lambda$ ein Vielfaches der Anzahl der Formen, welche die Periode von Φ_0 enthält, also eine gerade Zahl, so ist auch $2g + 2h + \nu + \lambda$ eine gerade Zahl, welche, durch die Anzahl der Formen der Periode von φ_0 dividirt, den Rest $2m$ geben möge. Es sind dann die Zahlen

$$K_{\nu+\lambda},\ K_{\nu+\lambda+1},\ K_{\nu+\lambda+2},\ \ldots$$

oder, was dasselbe ist,

$$K_0,\ K_1,\ K_2,\ \ldots$$

mit den Zahlen k_{2m}, k_{2m+1}, k_{2m+2}, ... identisch, d. h. es ist

$$\Omega_0 = (k_{2m},\ k_{2m+1},\ \ldots) = \omega_{2m},$$

und da aus der Identität der Wurzeln Ω_0, ω_{2m} sich die Identität der Formen Φ_0, φ_{2m} ergiebt, so haben wir bewiesen, dass die Form Φ_0 ein Glied der Periode von φ_0 ist.

Formen verschiedener Perioden können also nicht äquivalent sein.

Anmerkung. Nach § 99 ist eine Form ihrem Gefährten uneigentlich äquivalent. Wenn daher f und F zwei uneigentlich äquivalente reducirte Formen sind und G der Gefährte von F ist, so sind f und G eigentlich äquivalent; also muss

sich G in der Periode von f vorfinden. Sind nun f und F auf beide Arten äquivalent, so ist sowohl F, als auch G in der Periode von f enthalten; diese Periode ist also ihr eigener Gefährte und enthält zwei ambige Formen.

Aufgabe. Es sind zwei beliebige Formen Φ, φ einer positiven nichtquadratischen Determinante D gegeben. Man soll untersuchen, ob und in welcher Art dieselben äquivalent seien.

Lösung. Man ermittle eine reducirte Form F, welche eigentlich äquivalent Φ ist, und ebenso eine reducirte Form f, die φ äquivalent ist. Dann werden Φ, φ zu einander dieselbe Beziehung haben, wie F und f. Um diese letztere zu finden, bestimmen wir die Periode von f. Befindet sich in dieser Periode die Form F, aber nicht auch ihr Gefährte, so findet nur eigentliche Aequivalenz statt. Enthält die Periode von f nur den Gefährten von F (nicht F selbst), so findet nur uneigentliche Aequivalenz statt. Die Formen F, f und daher auch Φ, φ sind auf beide Arten äquivalent, wenn die Form F und zugleich ihr Gefährte der Periode von f angehören. Endlich sind die Formen nicht äquivalent, wenn weder die Form F, noch ihr Gefährte in der Periode von f vorhanden ist.

Beispiele. I. $D = 99$. Zu prüfende Formen: $(5, 13, 14)$, $(209, 473, 1070)$.

Ermittlung einer reducirten Form für jede derselben:

$$(5, 13, 14), (14, 1, -7), (-7, 6, 9).$$

$$(209, 473, 1070), (1070, -473, 209), (209, -154, 113),$$
$$(113, -72, 45), (45, -18, 5), (5, 8, -7).$$

Periode der ersteren reducirten Form:

$$(-7, 6, 9), (9, 3, -10), (-10, 7, 5), (5, 8, -7).$$

Resultat: Die Formen sind eigentlich äquivalent.

II. $D = 34$. Zu prüfende Formen:

$$(-75, 53, -37), (214, 240, 269).$$

Ermittlung einer reducirten Form für jede derselben:

$$(-75, 53, -37), (-37, -16, -6), (-6, 4, 3), (3, 5, -3).$$
$$(214, 240, 269), (269, 29, 3), (3, 4, -6).$$

Periode der ersteren reducirten Form:

(3, 5, −3), (− 3, 4, 6), (6, 2, − 5), (− 5, 3, 5),
(5, 2, − 6), (− 6, 4, 3).

Resultat: Die Formen sind uneigentlich äquivalent.

III. $D = 15$. Zu prüfende Formen: (10, 15, 21) und (− 179, − 391, − 854).

(10, 15, 21), (21, − 15, 10), (10, − 5, 1), (1, 3, − 6).
(− 179, − 391, − 854), (− 854, − 463, − 251),
(− 251, − 39, − 6), (− 6, 3, 1), (1, 3, − 6).

Die Formen sind auf beide Arten äquivalent.

IV. $D = 102$. Zu prüfende Formen: (11, 17, 17), (79, 24, 6).

(11, 17, 17), (17, 0, − 6), (− 6, 6, 11).
(79, 24, 6), (6, 6, − 11).

Periode der ersteren reducirten Form:

(− 6, 6, 11), (11, 5, − 7), (− 7, 9, 3), (3, 9, − 7),
(− 7, 5, 11), (11, 6, − 6).

Resultat: Die Formen sind nicht äquivalent.

§ 124. Transformation einer Form einer positiven nichtquadratischen Determinante in eine äquivalente Form. — Wir haben im vorigen Paragraphen die Frage der Aequivalenz zweier beliebigen Formen einer positiven nichtquadratischen Determinante D zum Abschluss gebracht. Auch haben wir in § 120 eine reducirte Form in eine andere Form derselben Periode transformirt. Es liegt uns jetzt ob, eine beliebige Form von D in eine beliebige äquivalente Form zu transformiren.

Es sei also Φ_0 eine beliebige Form der Determinante D und

(1) $$\Phi_0, \Phi_1, \Phi_2, \ldots, \Phi_n$$

die Reihe der äquivalenten Formen, deren letztes Glied Φ_n reducirt ist. Ferner sei φ_0 eine Φ_0 äquivalente Form und

(2) $$\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_\nu$$

die Reihe der äquivalenten Formen, deren letztes Glied φ_ν

ebenfalls reducirt ist. Wir bilden jetzt die Periode der Form $\varphi_\nu = f_0$

(3) $$f_0, f_1, f_2, \ldots, f_{2m-1}.$$

Da Φ_0 und φ_0 eigentlich äquivalent sind, so muss sich Φ_n in dieser Periode vorfinden. Angenommen, es sei $\Phi_n = f_k$, so lässt sich die Periode von f_0 folgendermassen schreiben:

$$f_0, f_1, f_2, \ldots, f_{k-1}, \Phi_n, f_{k+1}, \ldots, f_{2m-1}.$$

Wenn wir nun die Formen, welche den Gefährten von Φ_0, $\Phi_1, \ldots$ entgegengesetzt sind, beziehungsweise mit $\Psi_0, \Psi_1, \ldots$ bezeichnen, so ist

(4) $$\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_{\nu-1}, f_0, f_1, \ldots, f_{k-1}, \Psi_{n-1}, \Psi_{n-2}, \ldots, \Psi_0, \Phi_0$$

eine Reihe von Formen, von denen jede der folgenden nach links benachbart ist, und wir können somit auf die in § 110 dargelegte Weise eine eigentliche Transformation der ersten in die letzte ermitteln.

Dass jede Form wirklich der folgenden nach links benachbart sei, bedarf nur für die beiden Formen f_{k-1}, Ψ_{n-1} eines Beweises.

Es sei $f_{k-1} = (a, b, -a_1)$. Da nun auf f_{k-1} in der Periode von f_0, wie wir voraussetzen, Φ_n folgt, so wird

$$\Phi_n = (-a_1, ka_1 - b, a_2),$$

also

$$\Phi_{n-1} = (a_3, b + k'a_1, -a_1)$$

gesetzt werden können. Es ist somit

$$\Psi_{n-1} = (-a_1, -b - k'a_1, a_3),$$

und diese Form ist offenbar $(a, b, -a_1)$ nach rechts benachbart.

Beispiel. I. Die Form (5, 13, 14) in die äquivalente Form (209, 473, 1070) zu transformiren.

Die Reihen (1), (2), (3) sind oben angegeben.

Die Reihe (4) lautet

$$(5, 13, 14), (14, 1, -7), (-7, 6, 9), (9, 3, -10),$$
$$(-10, 7, 5), (5, 18, 45), (45, 72, 113), (113, 154, 209),$$
$$(209, 473, 1070).$$

Es ist also

$h_1 = 1$	$h_2 = -1$	$h_3 = 1$	$h_4 = -1$	$h_5 = 5$	$h_6 = 2$
0	-1	1	2	-3	-17
1	1	-2	-3	5	28

$h_7 = 2$	$h_8 = 3$	
-31	-45	-104
51	74	171

und die gesuchte Substitution ist

$$\begin{cases} x = -45x' - 104y' \\ y = 74x' + 171y'. \end{cases}$$

Wenn die Formen φ_0 und Φ_0 uneigentlich äquivalent sind, so ist φ_0 der Φ_0 entgegengesetzten Form eigentlich äquivalent, kann also in diese durch eine eigentliche Substitution

$$\begin{cases} x = \alpha x_1 + \beta y_1 \\ y = \gamma x_1 + \delta y_1 \end{cases}$$

transformirt werden. Dann wird aber φ_0 in Φ_0 selbst offenbar durch die uneigentliche Substitution

$$\begin{cases} x = \alpha x_1 - \beta y_1 \\ y = \gamma x_1 - \delta y_1 \end{cases}$$

transformirt.

Wenn somit φ_0, Φ_0 auf beide Arten äquivalent sind, so lassen sich nach dem Vorhergehenden zwei Transformationen der einen in die andere, eine eigentliche und eine uneigentliche, ermitteln.

Beispiel II. Die Form (10, 15, 21) soll in

$$(-179, -391,, -854)$$

transformirt werden; beide Formen sind, wie sich oben gezeigt hat, auf beide Arten äquivalent.

1. Ermittlung der eigentlichen Transformation. Die Reihen (1), (2), (3) sind oben angegeben. Reihe (4) lautet

(10, 15, 21), (21, − 15, 10), (10, − 5, 1), (1, − 3, − 6),

(— 6, 39, — 251), (— 251, 463, — 854), (— 845, 391, — 179),
(— 179, — 391, — 854).

Es ist also

$h_1 = 0$	$h_2 = -2$	$h_3 = -8$	$h_4 = -6$	$h_5 = -2$
0	-1	2	-15	88
1	0	-1	8	-47

$h_6 = -1$	$h_7 = 0$	
-161	73	161
86	-39	-86

und
$$\begin{cases} x = 73x_1 + 161y_1 \\ y = -39x_1 - 86y_1 \end{cases}$$
die gesuchte Transformation.

2. Ermittlung der uneigentlichen Transformation. Die der Form (— 179, — 391, — 854) entgegengesetzte Form liefert als Reihe (1)

(— 179, 391, — 854), (— 854, — 391, — 179),
(— 179, — 146, — 119), (— 119, — 92, — 71),
(— 71, — 50, — 35), (— 35, — 20, — 11), (— 11, — 2, 1),
(1, 3, — 6).

Die Reihe (4) lautet also

(10, 15, 21), (21, — 15, 10), (10, — 5, 1), (1, 2, — 11),
(— 11, 20, — 35), (— 35, 50, — 71), (— 71, 92, — 119),
(— 119, 146, — 179), (— 179, 391, — 854).

und man erhält

$h_1 = 0$	$h_2 = -2$	$h_3 = -3$	$h_4 = -2$	$h_5 = -2$
0	-1	2	-5	8
1	0	-1	3	-5

$h_6 = -2$	$h_7 = -2$	$h_8 = -3$	
-11	14	-17	37
7	-9	11	-24

(10, 15, 21) geht also über in (— 179, 391, — 854) durch die eigentliche Substitution

$$x = -17x_1 + 37y_1\,,\; y = 11x_1 - 24y_1$$

und daher in (— 179, — 391, — 854) durch die uneigentliche Substitution

$$\begin{cases} x = -17x_1 - 37y_1 \\ y = +11x_1 + 24y_1\,. \end{cases}$$

§ 125. Auflösung der Gleichung $t^2 - Du^2 = m^2$, wo D die Determinante der Form (M, N, P) und m der grösste gemeinschaftliche Divisor der Zahlen M, $2N$, P ist. — Wir haben uns jetzt, nachdem wir eine Transformation von φ_0 in Φ_0 ermittelt haben, mit der Auflösung der Pell'schen Gleichung zu beschäftigen, um mittels der Lösungen derselben alle übrigen Transformationen zu bestimmen. Von der auf der Hand liegenden Lösung $t = \pm m$, $u = 0$ abstrahirend, suchen wir zunächst die kleinsten positiven Zahlen, welche der Gleichung genügen, und aus der so gefundenen Lösung leiten wir sodann die übrigen Lösungen her.

1. Kleinste positive Lösung der Pell'schen Gleichung. — Wir nehmen eine (M, N, P) äquivalente reducirte Form $f_0 = (a, b, -a_1)$, in welcher a positiv ist, so dass auch die erste Wurzel ω_0 einen positiven Werth hat. Nach § 99 wird der grösste gemeinschaftliche Divisor von a, $2b$, a_1 gleichfalls m sein. Wir bilden jetzt die Periode von f_0, die aus $2g$ Gliedern bestehen möge, und berechnen nach § 120 die Grössen $h_1, h_2, h_3, \ldots, h_{2g}$. Dann ist nach § 122

$$\omega_0 = (h_1, h_2, h_3, \ldots, h_{2gn}, \omega_0),$$

wo jede Zahl h positiv zu nehmen und n irgend eine ganze positive Zahl ist.

Bilden wir nun die Näherungsbrüche dieses Kettenbruchs und nennen den h_{2gn} entsprechenden $\frac{\gamma}{\alpha}$, den folgenden $\frac{\delta}{\beta}$, so erhalten wir das Schema:

h_1	h_2	h_3	$\cdots$	h_{2gn}	ω_0	
$\frac{1}{0}$	$\frac{h_1}{1}$	$\frac{h_1 h_2 + 1}{h_2}$	$\cdots$	$\frac{\gamma}{\alpha}$	$\frac{\delta}{\beta}$	$\frac{\gamma + \delta\omega_0}{\alpha + \beta\omega_0}$.

Danach ist der Werth des ganzen Kettenbruchs $\omega_0 = \frac{\gamma + \delta\omega_n}{\alpha + \beta\omega_n}$, und da ausserdem $\frac{\delta}{\beta}$ ein Näherungsbruch gerader Ordnung, also $\alpha\delta - \beta\gamma = +1$ ist, so ist nach § 121, Lehrsatz II

$$\begin{cases} x = \alpha x_1 + \beta y_1 \\ y = \gamma x_1 + \delta y_1 \end{cases}$$

eine Substitution, welche f_0 in sich selbst transformirt.

Setzen wir daher für n der Reihe nach die Werthe 1, 2, 3, ..., so entspricht jedem derselben eine Transformation von f_0 in sich selbst. Die vier Zahlen α, β, γ, δ sind immer positiv, und da bei wachsendem n auch die Näherungsbrüche des Kettenbruchs wachsen, so liefern zwei verschiedene Werthe von n auch zwei verschiedene Substitutionen.

Umgekehrt lässt sich auch zeigen, dass auf die dargelegte Weise jede Transformation von f_0 in sich selbst erhalten wird, deren Coefficienten α, β, γ, δ positive Zahlen sind. Ist nämlich

$$x = \alpha x_1 + \beta y_1, \; y = \gamma x_1 + \delta y_1$$

eine Substitution, welche f_0 in sich selbst transformirt, so bestehen nach § 121, Lehrsatz I die beiden Gleichungen

$$\alpha\delta - \beta\gamma = 1 \quad \text{und} \quad \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

in welcher letzteren ω sowohl die erste, als auch die zweite Wurzel von f_0 sein kann. Wird die letzte Gleichung auf die Form

$$\beta\omega^2 + (\alpha - \delta)\omega - \gamma = 0$$

gebracht, so wird die linke Seite, da die eine Wurzel nach § 121 zwischen $+1$ und $+\infty$, die andere zwischen 0 und -1 liegt, für $\omega = +1$ negativ, für $\omega = -1$ positiv sein. Es ist also

$$\beta + \alpha - \delta - \gamma < 0, \; \beta - \alpha + \delta - \gamma > 0,$$

d. h.

$$\beta - \delta - (\gamma - \alpha) < 0, \; \delta - \gamma - (\alpha - \beta) > 0,$$

oder

$$\gamma - \alpha > \beta - \delta \quad \text{und} \quad \delta - \gamma > \alpha - \beta.$$

Hieraus ergiebt sich **erstens**, dass $\delta > \gamma$ ist. Wäre nämlich $\delta < \gamma$, so würde, weil $\alpha\delta = \beta\gamma + 1$, also $\alpha\delta > \beta\gamma$

ist, $\alpha > \beta$, also $\alpha - \beta > 0$ und um so mehr $\delta - \gamma > 0$, d. h. $\delta > \gamma$ sein müssen.

Zweitens lässt sich leicht nachweisen, dass $\gamma > \alpha$ ist. Wäre nämlich $\alpha > \gamma$ und zugleich $\delta > \beta$, so könnte die Gleichung $\alpha\delta - \beta\gamma = 1$ nicht statthaben; wenn wir nämlich $\alpha = \gamma + r$, $\delta = \beta + r'$ annehmen, wo also jede der Grössen $\alpha, \beta, \gamma, \delta, r, r'$ mindestens gleich 1 ist, so wird

$$\alpha\delta = \beta\gamma + \beta r + \gamma r' + rr',$$

d. h. $\alpha\delta$ um mindestens drei Einheiten grösser als $\beta\gamma$ sein. Die Annahme $\alpha > \gamma$ und zugleich $\delta > \beta$ ist also unstatthaft.

Wäre nun $\alpha > \gamma$ und zugleich $\delta \leqq \beta$, so wäre $\beta - \delta \geqq 0$, also würde die erste unserer beiden Ungleichungen $\gamma > \alpha$ liefern. Es kann also überhaupt nicht $\alpha > \gamma$ sein, und somit ist $\gamma \geqq \alpha$, $\delta > \gamma$.

Dies vorausgesetzt, lehrt der Hilfssatz des § 123, dass sich ω in den Kettenbruch

$$\omega = (\lambda, \mu, \ldots, \varrho, \sigma, \omega)$$

entwickeln lässt, wo die Grössen $\lambda, \mu, \ldots, \varrho, \sigma$ in gerader Anzahl vorhanden und jedenfalls $\mu, \ldots, \varrho$ positiv sind. Wir wollen nun zeigen, dass unter den gemachten Voraussetzungen auch λ und σ positive Zahlen sind.

Ist $\alpha = 1$, so geht dies sofort aus den in § 123 gemachten Voraussetzungen hervor, da dann $\lambda = \gamma$ und $\sigma = \beta$ ist, während die Zwischenglieder fehlen.

Ist ferner $\alpha > 1$, so leuchtet ein, dass jedenfalls λ als die grösste in $\frac{\gamma}{\alpha}$ enthaltene ganze Zahl positiv sein muss. Wir haben also nur zu zeigen, dass auch σ positiv sein wird. Zu diesem Zwecke wollen wir die unvollständigen Quotienten und die zugehörigen Näherungswerthe des für ω erhaltenen Kettenbruchs ins Auge fassen:

λ	μ	ν	$\ldots$	ϱ	σ	ω	
$\frac{1}{0}$	$\frac{\lambda}{1}$	$\frac{\mu\lambda+1}{\mu}$	$\ldots$	$\frac{Z_{2k}}{N_{2k}}$	$\frac{\gamma}{\alpha}$	$\frac{\delta}{\beta}$	ω

Da λ positiv ist, so sind die Zähler aller Näherungsbrüche positiv und bilden, wenigstens bis γ, eine steigende

Reihe, so dass $\gamma > Z_{2k}$ ist. Nun ist $\delta = \gamma\sigma + Z_{2k}$. Wäre also $\sigma = 0$, so müsste $\delta = Z_{2k}$, also $\delta < \gamma$ sein, was als unmöglich nachgewiesen ist.

Wäre ferner σ negativ, so würde auch $\gamma\sigma$ negativ sein, und da $|\gamma\sigma| > Z_{2k}$ ist, so wäre auch δ der Voraussetzung zuwider eine negative Zahl. Der Kettenbruch

$$\omega = (\lambda, \mu, \ldots, \varrho, \sigma, \omega)$$

hat somit nur positive Glieder, und die Anzahl der Grössen $\lambda, \mu, \ldots, \varrho, \sigma$ ist, wie schon bemerkt, eine gerade.

Andererseits erhält man für die Wurzel ω den rein periodischen Kettenbruch (mit positiven Gliedern)

$$\omega = (h_1, h_2, \ldots, h_{2n}, \omega),$$

und da beide Entwicklungen identisch sein müssen, so wird die Reihe der Zahlen

$$\lambda, \mu, \ldots, \varrho, \sigma$$

eine oder mehrere Perioden $h_1, \ldots, h_{2n}$ umfassen, und die Brüche $\frac{\gamma}{\alpha}, \frac{\delta}{\beta}$ werden zwei auf einander folgende Näherungsbrüche sein, welche dem Ende einer Periode entsprechen. Es ist also bewiesen, dass unser Verfahren auch jede Transformation (von f_0 in sich selbst) liefert, deren Coefficienten α, β, γ, δ positiv sind.

Da $\alpha, \beta, \gamma, \delta$ offenbar wachsen, wenn man von dem Ende der einen Periode zu dem der folgenden geht, so werden die kleinsten positiven Substitutionscoefficienten dem Ende der ersten Periode entsprechen.

Ebenso überzeugt man sich leicht, dass die kleinsten Werthe von $\alpha, \beta, \gamma, \delta$ aus den kleinsten Werthen von t und u erhalten werden. Da nämlich $f_0 = (a, b, -a_1)$ in sich selbst transformirt wird durch die beiden Substitutionen

$$\begin{cases} x = 1 \cdot x_1 + 0 \cdot y_1 \\ y = 0 \cdot x_1 + 1 \cdot y_1 \end{cases} \quad \text{und} \quad \begin{cases} x = \alpha x_1 + \beta y_1 \\ y = \gamma x_1 + \delta y_1, \end{cases}$$

so ist nach § 103

$$\alpha = \frac{t - bu}{m}, \quad \beta = \frac{a_1 u}{m}, \quad \gamma = \frac{au}{m}, \quad \delta = \frac{t + bu}{m}.$$

Daraus folgt

$$\alpha\delta = \frac{t^2 - b^2u^2}{m^2} = \frac{t^2 - Du^2}{m^2} + \frac{aa_1u^2}{m^2} = 1 + \frac{aa_1u^2}{m^2}.$$

und da die rechte Seite positiv ist, so müssen α und δ das selbe Zeichen haben. Nun ist aber $\alpha + \delta = \frac{2t}{m}$, also haben α, δ das Zeichen von t. Ebenso geht aus den Werthen von β, γ hervor, dass, wenn sie nicht beide Null sind, was $u = 0$ voraussetzt, sie dasselbe Zeichen wie u haben. Die oben untersuchten positiven Substitutionscoefficienten α, β, γ, δ werden also aus positiven Werthen t, u erhalten, und da β, γ mit u wachsen, so entsprechen die kleinsten Substitutionscoefficienten den kleinsten positiven Werthen von t, u. Diese letzteren, die wir mit T, U bezeichnen wollen, werden, sobald α, β, γ, δ durch die Kettenbruch-Entwicklung ermittelt sind, mittels der Formeln

$$T = \frac{(\alpha + \delta)m}{2}, \quad U = \frac{(\delta - \alpha)m}{2b}$$

gefunden.

Beispiele. I. Für die Form (20, 24, 24) ist $D = 96$, $m = 4$. Der gegebenen Form äquivalent ist die reducirte Form (8, 8, — 4) mit zweigliedriger Periode. Diese in sich selbst zu transformiren, schreiben wir

$$(8,\ 8,\ -4),\ (-4,\ 8,\ 8),\ |\ (8,\ 8,\ -4).$$

Es ist also

$$[h_1] = 4,\ h_2 = 2,$$

$$\begin{array}{c|c|c} 4 & 2 & \\ \frac{1}{0} & \frac{4}{1} & \frac{9}{2} \end{array}, \quad \begin{array}{l} \alpha = 1,\ \gamma = 4, \\ \beta = 2,\ \delta = 9 \end{array}$$

und
$$T = \frac{(1 + 9)4}{2} = 20,\ U = \frac{(9 - 1)4}{2 \cdot 8} = 2$$

die kleinste positive Auflösung der Gleichung $t^2 - 96u^2 = 16$.

II. Ausgangsform (15, 12, 6), $D = 54$, $m = 3$, Gleichung $t^2 - 54u^2 = 9$.

$$(6,\ 6,\ -3),\ (-3,\ 6,\ 6),\ |\ (6,\ 6,\ -3).$$

$$\begin{array}{c|c|c} [h_1] = 4 & h_2 = 2 & \\ \frac{1}{0} & \frac{4}{1} & \frac{9}{2} \end{array}, \quad \begin{array}{l} \alpha = 1,\ \gamma = 4 \\ \beta = 2,\ \delta = 9, \end{array}$$

$$T = \frac{(1 + 9)3}{2} = 15,\ U = \frac{(9 - 1)3}{2 \cdot 6} = 2.$$

III. Ausgangsform $(2, -3, -28)$, $D = 65$, $m = 2$, Gleichung $t^2 - 65u^2 = 4$.

$$(8, 1, -8), (-8, 7, 2), (2, 7, -8), (-8, 1, 8),$$
$$(8, 7, -2), (-2, 7, 8), | (8, 1, -8).$$

$\|h_1\| = 1$	$h_2 = 7$	$\|h_3\| = 1$	$h_4 = 1$	$\|h_5\| = 7$	$h_6 = 1$	
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{8}{7}$	$\frac{9}{8}$	$\frac{17}{15}$	$\frac{128}{113}$	$\frac{145}{128}$,

$$\alpha = 113, \beta = 128, \gamma = 128, \delta = 145,$$
$$T = 258, U = 32.$$

IV. $t^2 - 20u^2 = 4$ $[T = 18, U = 4]$.

V. $t^2 - 69u^2 = 1$ $[T = 7775, U = 936]$.

VI. $t^2 - 33u^2 = 1$ $[T = 23, U = 4]$.

VII. $t^2 - 70u^2 = 1$ $[T = 251, U = 30]$.

VIII. $t^2 - 115u^2 = 1$ $[T = 1126, U = 105]$.

2. Die übrigen Lösungen der Pell'schen Gleichung. Aus der kleinsten positiven Auflösung lassen sich die übrigen Lösungen leicht herleiten.

Da $T^2 - DU^2 = m^2$ oder

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right) = 1$$

ist, so ist auch, wenn e eine ganze Zahl bezeichnet,

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e \cdot \left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e = 1.$$

Wir behaupten nun, dass die Ausdrücke

$$(1)\quad \begin{cases} t_e = \frac{m}{2}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e + \frac{m}{2}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e \\ u_e = \frac{m}{2\sqrt{D}}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e - \frac{m}{2\sqrt{D}}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e \end{cases}$$

alle Lösungen unserer Gleichung liefern, wenn für e alle Zahlen 0, 1, 2, 3, ... gesetzt werden. [Es ist $t_0 = m$, $u_0 = 0$; $t_1 = T$, $u_1 = U$].

Dies zu beweisen, haben wir erstens darzuthun, dass die Werthe (1) für jede ganze positive Zahl e der Gleichung genügen.

Setzen wir für einen Augenblick

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e = \alpha, \ \left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e = \beta,$$

so ist $\alpha\beta = 1$, und wir erhalten

$$t_e = \frac{m}{2}(\alpha + \beta), \ u_e = \frac{m}{2\sqrt{D}}(\alpha - \beta),$$

$$t_e^2 = \frac{m^2}{4}(\alpha^2 + 2 + \beta^2), \ u_e^2 = \frac{m^2}{4D}(\alpha^2 - 2 + \beta^2),$$

also

$$t_e^2 - Du_e^2 = \frac{2m^2}{4} + \frac{2m^2}{4} = m^2,$$

woraus hervorgeht, dass t_e, u_e für jedes e der Gleichung

$$t^2 - Du^2 = m^2$$

genügen.

Zweitens haben wir zu zeigen, dass die Ausdrücke (1) für alle Werthe von e ganze Zahlen liefern. Wir setzen für einen Augenblick

$$\frac{T}{m} + \frac{U}{m}\sqrt{D} = \alpha', \ \frac{T}{m} - \frac{U}{m}\sqrt{D} = \beta',$$

so ist

$$t_{e-1} = \frac{m}{2}(\alpha'^{e-1} + \beta'^{e-1}), \ t_{e+1} = \frac{m}{2}(\alpha'^{e+1} + \beta'^{e+1}),$$

also

$$t_{e+1} + t_{e-1} = \frac{m}{2}(\alpha'^{e+1} + \alpha'^{e-1} + \beta'^{e+1} + \beta'^{e-1})$$

$$= \frac{m}{2}\left[\alpha'^e\left(\alpha' + \frac{1}{\alpha'}\right) + \beta'^e\left(\beta' + \frac{1}{\beta'}\right)\right].$$

Da aber $\alpha'\beta' = 1$, also $\frac{1}{\alpha'} = \beta'$ und $\frac{1}{\beta'} = \alpha'$ ist, so ergiebt sich

$$\alpha' + \frac{1}{\alpha'} = \beta' + \frac{1}{\beta'} = \alpha' + \beta' = \frac{2T}{m},$$

und es ist

$$t_{e+1} + t_{e-1} = \frac{m}{2} \cdot \frac{2T}{m}(\alpha'^e + \beta'^e)$$

oder, da

$$\frac{m}{2}(\alpha'^e + \beta'^e) = t_e$$

ist,

$$(2) \qquad t_{e+1} + t_{e-1} = \frac{2T}{m} t_e.$$

Auf genau dieselbe Weise erhalten wir

$$(3) \qquad u_{r+1} + u_{r-1} = \frac{2T}{m} u_r.$$

Nun ist

$$T^2 - DU^2, \text{ d. i. } T^2 - (N^2 - MP)U^2 = m^2,$$

also

$$4T^2 = 4m^2 + (4N^2 - 4MP)U^2,$$

und da die rechte Seite dieser Gleichung durch m^2 theilbar ist, so muss auch $4T^2$ durch m^2 theilbar oder $\frac{2T}{m}$ eine ganze (positive) Zahl sein. Wenn dies aber der Fall ist, so lehren die Gleichungen (2) und (3), dass jede der beiden Reihen

$$(4) \qquad \begin{cases} t_0 = m,\ t_1 = T,\ t_2,\ t_3,\ \ldots \\ u_0 = 0,\ u_1 = U,\ u_2,\ u_3,\ \ldots \end{cases}$$

nur ganze positive Zahlen enthält, von denen jede folgende grösser ist, als die vorhergehende.

Endlich haben wir noch darzuthun, dass es keine Lösung der Gleichung $t^2 - Du^2 = m^2$ in ganzen positiven Zahlen giebt, welche nicht durch die Ausdrücke (1) dargestellt wird. Angenommen, $\mathfrak{T}$, $\mathfrak{u}$ sei eine solche Lösung, so muss $\mathfrak{u}$ zwischen zwei auf einander folgenden Gliedern u_n, u_{n+1} der zweiten Reihe (4) liegen, so dass

$$u_{n+1} > \mathfrak{u} > u_n$$

ist. Bilden wir jetzt die Ausdrücke

$$t' = \frac{1}{m}(\mathfrak{T} t_n - D\mathfrak{u} u_n), \quad u' = \frac{1}{m}(\mathfrak{u} t_n - \mathfrak{T} u_n),$$

so ergiebt die wirkliche Berechnung, dass

$$t'^2 - Du'^2 = \frac{1}{m^2}(t_n^2 - Du_n^2)(\mathfrak{T}^2 - D\mathfrak{u}^2) = m^2,$$

dass also auch t', u' eine Lösung unserer Gleichung ist.

t', u' sind aber ganze Zahlen. Da nämlich

$$\mathfrak{T}^2 - D\mathfrak{u}^2, \text{ d. i. } \mathfrak{T}^2 - (N^2 - MP)\mathfrak{u}^2 = m^2,$$

oder

$$\mathfrak{T}^2 - N^2\mathfrak{u}^2 = m^2 - MP\mathfrak{u}^2$$

ist, und da die rechte Seite der letzten Gleichung den Factor m^2 enthält, so muss auch $\mathfrak{T}^2 - N^2\mathfrak{u}^2$ durch m^2, also jedenfalls $\mathfrak{T} + N\mathfrak{u}$ durch m theilbar sein. Ebenso erkennt man, dass $t_n + Nu_n$ durch m theilbar ist. Es ist also auch

$$\mathfrak{u}(t_n + N u_n) - u_n(\mathfrak{T} + N\mathfrak{u}) = \mathfrak{u} t_n - \mathfrak{T} u_n$$

ein Vielfaches von m, d. h.

$$u' = \frac{1}{m}(\mathfrak{u} t_n - \mathfrak{T} u_n)$$

eine ganze Zahl. Dann muss aber der Gleichung $t'^2 = Du'^2 + m^2$ wegen auch t' eine ganze Zahl sein. Wir haben also aus der angenommenen Lösung $\mathfrak{T}$, $\mathfrak{u}$ eine neue Lösung in ganzen Zahlen t', u' hergeleitet und wollen jetzt mittels der letzteren zeigen, dass unsere Annahme zu einem Widerspruch führt.

Zunächst leuchtet ein, dass u' nicht Null sein kann. Wäre nämlich $u' = 0$, also

$$\mathfrak{u} t_n = \mathfrak{T} u_n, \quad \mathfrak{u}^2 t_n^2 = \mathfrak{T}^2 u_n^2,$$

so müsste, da

$$\mathfrak{T}^2 = D\mathfrak{u}^2 + m^2, \quad t_n^2 = Du_n^2 + m^2$$

ist,

$$\mathfrak{u}^2 (Du_n^2 + m^2) = (D\mathfrak{u}^2 + m^2) u_n^2$$

sein, und hieraus würde sich $\mathfrak{u} = u_n$ ergeben, während doch $\mathfrak{u} > u_n$ vorausgesetzt wird. Daher ist $u' > 0$ und da, wie wir bewiesen haben, U der kleinste positive Werth von u ist, so ist $u' > U$.

Setzen wir jetzt wieder

$$\frac{T}{m} + \frac{U}{m}\sqrt{D} = \alpha', \quad \frac{T}{m} - \frac{U}{m}\sqrt{D} = \beta',$$

so ist nach den Formeln (1)

$$u_{n+1} = \frac{m}{2\sqrt{D}}(\alpha'^{n+1} - \beta'^{n+1}), \quad u_n = \frac{m}{2\sqrt{D}}(\alpha'^n - \beta'^n),$$

$$t_{n+1} = \frac{m}{2}(\alpha'^{n+1} + \beta'^{n+1}), \quad t_n = \frac{m}{2}(\alpha'^n + \beta'^n),$$

und hieraus ergiebt sich

$$u_{n+1} t_n - t_{n+1} u_n = \frac{m^2}{4\sqrt{D}}(2\alpha'^{n+1}\beta'^n - 2\alpha'^n\beta'^{n+1})$$

$$= \frac{m^2}{2\sqrt{D}}\alpha'^n\beta'^n(\alpha' - \beta')$$

oder, da

$$\alpha' - \beta' = \frac{2U}{m}\sqrt{D} \quad \text{und} \quad \alpha'\beta' = 1$$

ist,

$$u_{n+1} t_n - t_{n+1} u_n = mU.$$

Da nun $u' = \frac{1}{m}(\mathfrak{U} t_n - \mathfrak{T} u_n)$ nicht kleiner als U, also $\mathfrak{U} t_n - \mathfrak{T} u_n$ nicht kleiner als $m U$ ist, so ist

$$\mathfrak{U} t_n - \mathfrak{T} u_n > u_{n+1} t_n - t_{n+1} u_n . \tag{5}$$

Ferner liefert die Gleichung $\mathfrak{T}^2 - D\mathfrak{U}^2 = m^2$

$$\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{D + \frac{m^2}{\mathfrak{U}^2}} .$$

Ebenso ist

$$\frac{t_{n+1}}{u_{n+1}} = \sqrt{D + \frac{m^2}{u_{n+1}^2}} .$$

Da nun $u_{n+1} > \mathfrak{U}$ vorausgesetzt wird, so ist

$$\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t_{n+1}}{u_{n+1}},$$

also auch

$$t_n + u_n \frac{\mathfrak{T}}{\mathfrak{U}} > t_n + u_n \frac{t_{n+1}}{u_{n+1}}$$

und mit Rücksicht auf (5)

$$(\mathfrak{U} t_n - \mathfrak{T} u_n)\left(t_n + u_n \frac{\mathfrak{T}}{\mathfrak{U}}\right) > (u_{n+1} t_n - t_{n+1} u_n)\left(t_n + u_n \frac{t_{n+1}}{u_{n+1}}\right)$$

oder

$$\mathfrak{U} t_n^2 - \frac{\mathfrak{T}^2 u_n^2}{\mathfrak{U}} > u_{n+1} t_n^2 - \frac{t_{n+1}^2 u_n^2}{u_{n+1}} .$$

Wird hierin

$$\mathfrak{T}^2 = D\mathfrak{U}^2 + m^2, \; t_n^2 = D u_n^2 + m^2, \; t_{n+1}^2 = D u_{n+1}^2 + m^2$$

gesetzt, so erhält man nach leichten Reductionen

$$\mathfrak{U} - \frac{u_n^2}{\mathfrak{U}} > u_{n+1} - \frac{u_n^2}{u_{n+1}}$$

oder

$$\mathfrak{U} + \frac{u_n^2}{u_{n+1}} > u_{n+1} + \frac{u_n^2}{\mathfrak{U}}, \tag{6}$$

und diese Ungleichung ist unmöglich, da $\mathfrak{U} < u_{n+1}$ und somit auch $\frac{u_n^2}{u_{n+1}} < \frac{u_n^2}{\mathfrak{U}}$ ist. Unsere Annahme, dass die Gleichung $t^2 - Du^2 = m^2$ Lösungen in ganzen positiven Zahlen habe, welche durch die Formeln (1) nicht dargestellt würden, ist somit falsch.

Was nun die Berechnung der übrigen Wurzeln der Gleichung

$$t^2 - Du^2 = m^2$$

betrifft, so geschieht dieselbe am zweckmässigsten vermittels der Formeln (2) und (3). Dies wollen wir noch an einem Beispiel zeigen. Wir fanden oben, dass die Gleichung

$$t^2 - 96u^2 = 16$$

die Lösung $T = 20$, $U = 2$ hat. Es ist also

$$\frac{2T}{m} = \frac{2 \cdot 20}{4} = 10,$$

und da ausserdem $t_0 = 4$, $u_0 = 0$ ist, so liefern die Formeln (2) und (3) zunächst

$$t_2 = 10 \cdot 20 - 4 = 196, \quad u_2 = 10 \cdot 2 - 0 = 20,$$

weiter

$$t_3 = 10 \cdot 196 - 20 = 1940, \quad u_3 = 10 \cdot 20 - 2 = 198,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

Dass aus jeder Lösung t, u in positiven Zahlen sich durch Aenderung der Vorzeichen noch drei andere Lösungen ergeben, braucht wohl nicht erst bemerkt zu werden.

§ 126. Darstellungen einer gegebenen Zahl M durch eine gegebene Form von positiver nichtquadratischer Determinante. — Der § 123 hat uns in den Stand gesetzt, zu entscheiden, ob zwei gegebene Formen einer positiven nichtquadratischen Determinante äquivalent seien oder nicht. Darauf haben wir in § 124 gesehen, wie man im ersteren Falle eine eigentliche Transformation der einen in die andere ermittelt. Endlich hat uns die Lösung der Pell'schen Gleichung das Mittel gegeben, aus dieser einen Transformation alle anderen gleichartigen herzuleiten. Nach den Entwicklungen des § 106 ist also die Aufgabe: „Alle eigentlichen Darstellungen einer gegebenen Zahl durch eine gegebene Form zu ermitteln“ auch für den Fall einer positiven nichtquadratischen Determinante als vollständig gelöst zu betrachten.

Zur besseren Einübung der gewonnenen Resultate mögen noch zwei Beispiele folgen.

I. Beispiel. Die Zahl $M = 673$ durch die Form (13, 15, 12) der Determinante 69 darzustellen, also die Gleichung

$$13x^2 + 30xy + 12y^2 = 673$$

in ganzen Zahlen zu lösen.

Die Congruenz $\xi^2 \equiv 69 \pmod{673}$ ist möglich und hat die Wurzeln ± 289.

1. Darstellungen, die zu $+289$ gehören.

$$(13,\ 15,\ 12),\ (12,\ -3,\ -5),\ (-5,\ 8,\ 1),\ (1,\ 8,\ -5).$$

$$(673,\ 289,\ 124),\ (124,\ -41,\ 13),\ (13,\ 2,\ -5),\ (-5,\ 8,\ 1).$$

Da beide Formen äquivalent sind, so ist die Darstellung möglich. Wir bilden nun die Reihe der benachbarten Formen

$$(13,\ 15,\ 12),\ (12,\ -3,\ -5),\ (-5,\ 8,\ 1),\ (1,\ -8,\ -5),$$
$$(-5,\ -2,\ 13),\ (13,\ 41,\ 124),\ (124,\ -289,\ 673),$$
$$(673,\ 289,\ 124).$$

Es ist somit

$h_1 = 1$	$h_2 = -1$	$h_3 = 0$	$h_4 = 2$	$h_5 = 3$
0	-1	1	1	1
1	1	-2	-1	0

$h_6 = -2$	$h_7 = 0$	
2	-5	-2
1	-2	-1

d. h. (13, 15, 12) geht in (673, 289, 124) durch die Substitution

$$\begin{cases} x = -5x_1 - 2y_1 \\ y = -2x_1 - y_1 \end{cases}$$

über. Es ist also

$$\begin{cases} x = \pm 5 \\ y = \pm 2 \end{cases}$$

eine erste eigentliche Darstellung von 673 durch die Form (13, 15, 12), und alle anderen zur Wurzel 289 gehörenden Darstellungen dieser Art werden nach § 106 durch die Formeln

$$x = 5t - 99u,\ y = 2t + 95u$$

geliefert, wenn darin für t, u alle Lösungen der (oben behandelten) Gleichung

$$t^2 - 69u^2 = 1$$

gesetzt werden.

2. Darstellungen, die zu -289 gehören.

$$(673,\ -289,\ 124),\ (124,\ -83,\ 55),\ (55,\ -27,\ 12),$$
$$(12,\ 3,\ -5),\ (-5,\ 7,\ 4),\ (4,\ 5,\ -11).$$

Reihe der benachbarten Formen:

$$(13,\ 15,\ 12),\ (12,\ -3,\ -5),\ (-5,\ 8,\ 1),\ (1,\ 8,\ -5),$$
$$(-5,\ -3,\ 12),\ (12,\ 27,\ 55),\ (55,\ 83,\ 124),\ (124,\ 289,\ 673),$$
$$(673,\ -289,\ 124).$$

Es ist also

$h_1 = 1$	$h_2 = -1$	$h_3 = 16$	$h_4 = -1$	$h_5 = 2$	$h_6 = 2$
0	-1	1	17	-18	-53
1	1	-2	-33	35	103

$h_7 = 3$	$h_8 = 0$	
-88	-211	88
171	410	-171

,

und dann liefern die Formeln

$$\begin{cases} x = -211t - (-211 \cdot 15 + 410 \cdot 12)u = -211t - 1755u \\ y = +410t + (-211 \cdot 13 + 410 \cdot 15)u = 410t + 3407u, \end{cases}$$

wenn für t, u alle Lösungen der Gleichung

$$t^2 - 69u^2 = 1$$

gesetzt werden, alle zur Wurzel -289 gehörenden eigentlichen Darstellungen von 673 durch die Form (13, 15, 12).

II. Beispiel. $4x^2 + 12xy - 14y^2 = 1106$.

Hier ist $D = 92$, $m = 2$, also lautet die Hülfsgleichung

$$t^2 - 92u^2 = 4,$$

und diese hat die Lösungen

t	2	48	$48 \cdot 48 - 2 = 2302$	$48 \cdot 2302 - 48$	$\cdots$
u	0	5	$48 \cdot 5 - 0 = 240$	$48 \cdot 240 - 5$	$\cdots$

Die Congruenz $\xi^2 \equiv 92 \pmod{1106}$ hat die 4 Wurzeln ± 48, ± 426.

1. Darstellungen, die zu + 48 gehören.

Reihe der benachbarten Formen:

(4, 6, — 14), (— 14, 8, 2), (2, — 48, 1106), (1106, 48, 2).

$h_1 = -1$	$h_2 = -20$	$h_3 = 0$	
0	-1	20	1
1	-1	19	1

Die hierher gehörigen Darstellungen werden also (§ 106) durch die Formeln

$$\begin{cases} x = \frac{1}{2}(20t + 146u) \\ y = \frac{1}{2}(19t + 194u) \end{cases}$$

geliefert, und die kleinsten Lösungen, welche diese enthalten, sind $x = 20$, $y = 19$; dann folgen $x = 845$, $y = 941$; u. s. w.

2. Darstellungen, die zu — 48 gehören.

Formenreihe:

(4, 6, — 14), (— 14, 8, 2), (2, 48, 1106), (1106, — 48, 2).

$h_1 = -1$	$h_2 = 28$	$h_3 = 0$	
0	-1	-28	1
1	-1	-29	1

Darstellungen:

$$\begin{cases} x = -\frac{1}{2}(28t + 238u) \\ y = -\frac{1}{2}(29t + 286u), \end{cases}$$

also
$$\begin{cases} x = \pm 28 \\ y = \pm 29 \end{cases}, \text{ u. s. w.}$$

3. Darstellungen, die zu + 426 gehören.

Formenreihe:

(4, 6, — 14), (— 14, — 6, 4), (4, 18, 58), (58, 98, 164), (164, — 426, 1106), (1106, 426, 164).

$h_1 = 0$	$h_2 = 3$	$h_3 = 2$	$h_4 = -2$	$h_5 = 0$	
0	-1	-3	-5	13	5
1	0	-1	-2	5	2

Darstellungen:

$$\begin{cases} x = \frac{1}{2}(13t - 8u) \\ y = \frac{1}{2}(5t + 82u), \end{cases}$$

also

$$\begin{cases} x = + 13 \\ y = + 5, \end{cases} \quad \text{u. s. w.}$$

4. Darstellungen, die zu -426 gehören.

Formenreihe:

$$(4, 6, -14), (-14, 8, 2), (2, 12, 26), (26, 66, 164),$$
$$(164, 426, 1106), (1106, -426, 164).$$

$h_1 = -1$	$h_2 = 10$	$h_3 = 3$	$h_4 = 3$	$h_5 = 0$	
0	-1	-10	-29	-77	29
1	-1	-11	-32	-85	32

Darstellungen:

$$\begin{cases} x = -\frac{1}{2}(77t + 728u) \\ y = -\frac{1}{2}(85t + 818u). \end{cases}$$

Für $t = 48$, $u = -5$ z. B. ist $x = -28$, $y = +5$.

Elftes Kapitel.

Formen, deren Determinante ein Quadrat oder gleich Null ist. Auflösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten.

§ 127. Reducirte Formen quadratischer Determinanten. — Ist die Determinante der Form (a, b, c) eine Quadratzahl, also $b^2 - ac = h^2$, so ist $h^2 - b^2 = - ac$; somit besteht die Proportion

$$h - b : a = c : -(h + b),$$

und darin soll h die positive Quadratwurzel aus h^2 bezeichnen.

Wir drücken jetzt das Verhältniss $h - b : a$ in den kleinsten Zahlen aus; wenn wir auf diese Weise

$$h - b : a = \beta : \delta$$

erhalten, wo also β prim zu δ ist, so bestimmen wir weiter zwei ganze Zahlen α, β, welche der Gleichung

$$\alpha\delta - \beta\gamma = +1$$

genügen, und transformiren die gegebene Form (a, b, c) vermittels der Substitution

$$x = \alpha x_1 + \beta y_1, \quad y = \gamma x_1 + \delta y_1.$$

Wird die so erhaltene, der gegebenen äquivalente Form mit (a_1, b_1, c_1) bezeichnet, so ist

$$a_1 = a\alpha^2 + 2b\alpha\gamma + c\gamma^2;$$
$$b_1 = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta$$

oder, da nach unserer Annahme

$$h - b : a = \beta : \delta, \text{ also } a\beta = \delta(h - b),$$

und ebenso

$$c : -(h + b) = \beta : \delta, \quad \text{also} \quad c\delta = -\beta(h + b)$$

ist,

$$b_1 = \alpha\delta(h - b) + b(\alpha\delta + \beta\gamma) - \beta\gamma(h + b)$$
$$= h(\alpha\delta - \beta\gamma) = h;$$
$$c_1 = a\beta^2 + 2b\beta\delta + c\delta^2 = \beta\delta(h - b) + 2b\beta\delta - \beta\delta(h + b) = 0.$$

Die Form (a, b, c) ist also in die äquivalente Form $(a_1, h, 0)$ übergegangen, wo a_1 den oben angegebenen Werth hat.

Liegt dieser Werth von a_1 ausserhalb der Grenzen 0 und $2h - 1$, so unterwerfen wir die Form $(a_1, h, 0)$ der neuen eigentlichen Substitution $x_1 = x_2$, $y_1 = kx_2 + y_2$, wo k eine vorläufig unbestimmte ganze Zahl bezeichnet. Dadurch erhalten wir eine dritte Form $(a_1 + 2hk, h, 0)$, welche der zweiten und daher auch der ersten äquivalent ist, und jetzt können wir über die Zahl k so verfügen, dass

$$0 < a_1 + 2hk < 2h - 1$$

werde. Die auf diese Weise gebildete Form $(a_2, h, 0)$, welche wir offenbar auch direkt aus der ersten durch die Substitution

$$\begin{cases} x = \alpha x_2 + \beta(kx_2 + y_2) = (\alpha + \beta k)x_2 + \beta y_2 \\ y = \gamma x_2 + \delta(kx_2 + y_2) = (\gamma + \delta k)x_2 + \delta y_2 \end{cases}$$

erhalten haben würden, wird hier eine reducirte Form genannt.

Beispiele. I. Die Form $(14, 8, 2)$ hat die Determinante 36. Es ist $6^2 - 8^2 = -2 \cdot 14$, also

$$(6 - 8) : 14 = 2 : -(6 + 8) = 1 : (-7).$$

Wir setzen demnach $\beta = 1$, $\delta = -7$ und bestimmen α und γ durch die Gleichung

$$-7\alpha - \gamma = 1.$$

Es ergiebt sich $\alpha = -1$, $\gamma = +6$, und da für diese Werthe $a_1 = 14 - 96 + 72 = -10$ wird, so erhalten wir die der gegebenen äquivalente Form $(-10, 6, 0)$.

Damit der Ausdruck $a_1 + 2hk = -10 + 12k$ zwischen 0 und 11 zu liegen komme, muss $k = 1$ angenommen werden. $(14, 8, 2)$ ist also äquivalent der reducirten Form $(2, 6, 0)$ und geht direkt in dieselbe über durch die Substitution

$$x = y_2, \quad y = -x_2 - 7y_2.$$

II. Die Form (4, 9, 8) der Determinante 49 geht durch die Substitution $x = y_1$, $y = -x_1 - y_1$ in die äquivalente reducirte Form (8, 7, 0) über.

Anmerkung. Man sieht sofort, dass es für eine Determinante h^2 genau $2h$ reducirte Formen giebt, da der erste Coefficient jeden der Werthe 0, 1, 2, . . ., $2h - 1$ haben kann.

§ 128. Aequivalenz der Formen mit quadratischer Determinante.

Lehrsatz. Zwei reducirte Formen einer quadratischen Determinante können nicht eigentlich äquivalent sein, wofern sie nicht identisch sind.

Beweis. Geht die reducirte Form $(a, h, 0)$ durch die eigentliche Substitution

$$x = \alpha x_1 + \beta y_1, \quad y = \gamma x_1 + \delta y_1$$

in die äquivalente reducirte Form $(a_1, h, 0)$ über, so bestehen die Gleichungen

$$(1) \qquad a_1 = a\alpha^2 + 2h\alpha\gamma,$$

$$(2) \qquad h = a\alpha\beta + h(\alpha\delta + \beta\gamma),$$

$$(3) \qquad 0 = a\beta^2 + 2h\beta\delta,$$

$$(4) \qquad \alpha\delta - \beta\gamma = 1.$$

Durch $(2).\beta - (3).\alpha$ ergiebt sich nun

$$-\beta h(\alpha\delta - \beta\gamma) = \beta h$$

oder wegen (4) $-\beta h = \beta h$, und da h von Null verschieden ist, so muss $\beta = 0$ sein.

Dann folgt aus (4) $\alpha\delta = 1$, also $\alpha = \delta = \pm 1$, und (1) geht über in

$$a_1 = a + 2h\gamma \quad \text{oder} \quad a_1 \equiv a \pmod{2h}.$$

Da aber jede der Zahlen a, a_1 zwischen 0 und $2h - 1$ liegt, so können dieselben nicht für den Modul $2h$ congruent sein, wofern sie nicht einander gleich sind, und dann sind die Formen $(a, h, 0)$ und $(a_1, h, 0)$ identisch.

Es hat jetzt nicht die geringste Schwierigkeit, zu entscheiden, ob zwei gegebene Formen einer quadratischen Determinante äquivalent seien oder nicht. Man braucht nämlich nur für jede der beiden die äquivalente reducirte Form zu

suchen. Wenn die beiden reducirten Formen, die man erhält, identisch sind, so sind die vorgelegten Formen äquivalent, sonst nicht.

Wie man durch Benutzung der Form, welche einer der beiden Formen entgegengesetzt ist, auch über etwa vorhandene uneigentliche Aequivalenz entscheidet, ist schon öfter dargelegt worden.

Beispiele. I. Die Formen (13, 17, 16), (91, 61, 40) der Determinante 81 sind eigentlich äquivalent; denn beide führen zu der reducirten Form (7, 9, 0), in welche die erste durch die Substitution

$$x = 3x_1 + 8y_1, \quad y = -5x_1 - 13y_1,$$

die zweite durch die Substitution

$$x = x_1 + 4y_1, \quad y = -2x_1 - 7y_1$$

transformirt wird.

II. Die Form (7, 12, 9) derselben Determinante 81 geht durch die Substitution

$$x = 2x_1 + 3y_1, \quad y = -5x_1 - 7y_1$$

in die reducirte Form (13, 9, 0) über, ist also (13, 17, 16) nicht eigentlich äquivalent.

Da jedoch (7, — 12, 9), wie sich leicht zeigen lässt, zur reducirten Form (7, 9, 0) führt, also (13, 17, 16) eigentlich äquivalent ist, so sind (7, 12, 9) und (13, 17, 16) uneigentlich äquivalent.

§ 129. Transformation einer Form einer quadratischen Determinante in eine äquivalente Form. — Es seien F und F_1 zwei eigentlich äquivalente Formen einer Determinante h^2, so lassen sich zwei eigentliche Substitutionen

$$(1) \qquad \begin{cases} x = \alpha x_1 + \beta y_1 \\ y = \gamma x_1 + \delta y_1 \end{cases}, \qquad (2) \qquad \begin{cases} x = \alpha_1 x_1 + \beta_1 y_1 \\ y = \gamma_1 x_1 + \delta_1 y_1 \end{cases}$$

ermitteln, von denen die erste F, die zweite F_1 in die reducirte Form φ transformirt. Da nun umgekehrt φ sich in F_1 verwandelt, wenn man

$$(3) \qquad \begin{cases} x_1 = \delta_1 x_2 - \beta_1 y_2 \\ y_1 = -\gamma_1 x_2 + \alpha_1 y_2 \end{cases}$$

setzt, so leuchtet ein, dass F in F_1 übergehen wird, wenn man die Substitutionen (1) und (3) nach einander oder direkt die Substitution

$$(4)\quad \begin{cases} x = \alpha(\delta_1 x_2 - \beta_1 y_2) + \beta(-\gamma_1 x_2 + \alpha_1 y_2) \\ \qquad = (\alpha\delta_1 - \beta\gamma_1)x_2 + (\beta\alpha_1 - \alpha\beta_1)y_2 \\ y = \gamma(\delta_1 x_2 - \beta_1 y_2) + \delta(-\gamma_1 x_2 + \alpha_1 y_2) \\ \qquad = (\gamma\delta_1 - \delta\gamma_1)x_2 + (\delta\alpha_1 - \gamma\beta_1)y_2 \end{cases}$$

anwendet.

Auf ähnliche Weise kann man auch eine Form in eine ihr uneigentlich äquivalente transformiren, und wenn zwei Formen auf beide Arten äquivalent sind, zwei Transformationen der einen in die andere herleiten, eine eigentliche und eine uneigentliche.

Beispiel. Die Form $F = (8, 15, 13)$ geht durch die Substitution $x = y_1$, $y = -x_1 - 2y_1$ in die reducirte Form $\varphi = (13, 11, 0)$ über. In dieselbe Form φ verwandelt sich $F_1 = (51, 130, 329)$ durch die Substitution $x = 2x_1 + 7y_1$, $y = -x_1 - 3y_1$; daher geht umgekehrt φ in F_1 über, wenn man $x_1 = -3x_2 - 7y_2$, $y_1 = x_2 + 2y_2$ setzt, und F in F_1 durch die Substitution

$$\begin{cases} x = y_1 = x_2 + 2y_2 \\ y = -(-3x_2 - 7y_2) - 2(x_2 + 2y_2) = x_2 + 3y_2. \end{cases}$$

§ 130. Auflösung der Gleichung $t^2 - h^2u^2 = m^2$. — In dem hier behandelten Falle einer quadratischen Determinante hat die Pell'sche Gleichung nur die beiden Lösungen $t = \pm m$, $u = 0$. Dies zu beweisen, nehmen wir an, es gäbe noch eine Lösung $t = T$, $u = U$, und es sei U von Null verschieden. Dann würde $\frac{4T^2}{m^2} - \frac{4h^2U^2}{m^2} = 4$ sein, und da m in $2h$, also m^2 in $4h^2$ aufgeht, so müsste offenbar auch $\frac{4T^2}{m^2}$ eine ganze Zahl sein. Wir hätten also zwei ganze Zahlen, deren Quadrate die Differenz 4 lieferten, und das ist unmöglich, wofern nicht eine der Zahlen Null ist.

Ist demnach

$$x = \alpha x_1 + \beta y_1, \qquad y = \gamma x_1 + \delta y_1$$

eine eigentliche Substitution, welche F in die eigentlich äquivalente Form F_1 transformirt, so sind nach § 103

$$\begin{cases} x = \frac{1}{m}(\pm \alpha m) x_1 + \frac{1}{m}(\pm \beta m) y_1 \\ y = \frac{1}{m}(\pm \gamma m) x_1 + \frac{1}{m}(\pm \delta m) y_1 \end{cases}$$

oder, was dasselbe ist,

$$\begin{cases} x = \pm \alpha x_1 \pm \beta y_1 \\ y = \pm \gamma x_1 \pm \delta y_1 \end{cases}$$

die Formeln, welche alle gleichartigen Substitutionen enthalten, die dieses leisten. Wenn also F und F_1 nur auf eine Art äquivalent sind, so giebt es nur zwei Transformationen der einen Form in die andere. Sind F und F_1 auf beide Arten äquivalent, so giebt es zwei eigentliche und zwei uneigentliche Transformationen.

§ 131. Darstellungen einer Zahl M durch eine Form (a, b, c) einer quadratischen Determinante k^2. —

1. Methode. Das oben für den Fall einer negativen oder einer positiven nichtquadratischen Determinante dargelegte Verfahren findet, wenn auch $b^2 - ac$ eine Quadratzahl ist, unverändert Anwendung, wie wir sofort an einem Beispiel zeigen wollen.

Aufgabe. Es soll die Gleichung

$$8x^2 + 26xy + 11y^2 = 585$$

in ganzen Zahlen gelöst werden. Da $585 = 5 . 9 . 13$ durch die Quadratzahl 9 theilbar ist, so werden möglicherweise eigentliche und uneigentliche Darstellungen, letztere von der Form $x = 3m$, $y = 3n$, vorhanden sein.

1. Ermittlung der uneigentlichen Darstellungen. Setzen wir $x = 3x_1$, $y = 3y_1$, so geht die vorgelegte Gleichung über in

$$8x_1^2 + 26x_1y_1 + 11y_1^2 = 65.$$

Die Determinante der Form $(8, 13, 11)$ ist 81, und die Congruenz

$$\xi^2 \equiv 81 \pmod{65}$$

hat die 4 Wurzeln ± 4, ± 9.

Die Formen $(65, \pm 4, 1)$ führen zu keinen Darstellungen, da sie der reducirten Form $(17, 9, 0)$ äquivalent sind, während $(8, 13, 11)$ der reducirten Form $(11, 9, 0)$ äquivalent ist.

Dagegen geht $(65, +9, 0)$ durch die Substitution $x_1 = x_2$, $y_1 = -3x_2 + y_2$ in $(11, 9, 0)$, also $(11, 9, 0)$ umgekehrt in $(65, 9, 0)$ über, wenn $x_2 = x_1$, $y_2 = 3x_1 + y_1$ gesetzt wird. Da nun $(8, 13, 11)$ durch die Substitution

$$x_1 = y_2, \qquad y_1 = -x_2 - 2y_2$$

in $(11, 9, 0)$ transformirt wird, so wird $(8, 13, 11)$ in $(65, 9, 0)$ verwandelt, wenn man erst

$$x_1 = y_2, \qquad y_1 = -x_2 - 2y_2$$

und sodann $x_2 = x_3$, $y_2 = 3x_3 + y_3$, oder direkt

$$\begin{cases} x_1 = 3x_3 + y_3 \\ y_1 = -7x_3 - 2y_3 \end{cases}$$

setzt.

Die Hülfsgleichung $t^2 - 81u^2 = 1$ hat nur die Lösungen $t = \pm 1$, $u = 0$, und somit ergeben sich die beiden Darstellungen

$$x_1 = \pm 3, \qquad y_1 = \mp 7,$$

denen die uneigentlichen Darstellungen

$$x = \pm 9, \qquad y = \mp 21$$

entsprechen.

Die Form $(65, -9, 0)$ ist $(8, 13, 11)$ nicht eigentlich äquivalent, liefert also keine Darstellung.

2. Ermittlung der eigentlichen Darstellungen. Die Congruenz

$$\xi^2 \equiv 81 \pmod{585}$$

hat die 12 Wurzeln

$$\pm 9, \quad \pm 69, \quad \pm 126, \quad \pm 186, \quad \pm 204, \quad \pm 264.$$

Nun sind die 9 Formen

$(585, \pm 9, 0)$, $(585, 69, 8)$, $(585, \pm 126, 27)$, $(585, -186, 59)$, $(585, \pm 204, 71)$, $(585, -264, 119)$

der Form $(8, 13, 11)$ nicht äquivalent, liefern also keine Darstellungen.

(585, — 69, 8) geht durch die Substitution

$$\begin{cases} x = x_1 + 2y_1 \\ y = 7x_1 + 15y_1 \end{cases}$$

in (11, 9, 0) über, letztere Form also in erstere durch die Substitution

$$\begin{cases} x_1 = 15x_2 - 2y_2 \\ y_1 = - 7x_2 + y_2 \end{cases},$$

und somit (8, 13, 11) in (585, — 69, 8) durch die Substitution

$$\begin{cases} x = - 7x_2 + y_2 \\ y = - x_2 \end{cases},$$

und dadurch erhalten wir die beiden eigentlichen Darstellungen $x = \pm 7$, $y = \pm 1$.

Ebenso liefert die Form (585, 186, 59) die beiden Darstellungen $x = \pm 119$, $y = \mp 43$, und die Form (585, 264, 119) die beiden Darstellungen $x = \pm 23$, $y = \mp 7$, so dass sich für die vorgelegte Gleichung im Ganzen folgende 8 Lösungen ergeben:

x	± 9	± 7	± 23	± 119
y	∓ 21	± 1	∓ 7	∓ 43

2. Methode. Bekanntlich sind die Wurzeln der Gleichung $a\omega^2 + 2b\omega + c = 0$, wenn $b^2 - ac = h^2$ ist, rational und liefern die rationale Zerlegung

$$a\omega^2 + 2b\omega + c = a\left(\omega - \frac{h-b}{a}\right)\left(\omega + \frac{h+b}{a}\right),$$

und hieraus folgt, wenn ω durch $\frac{x}{y}$ ersetzt und beiderseits mit y^2 multiplicirt wird,

$$ax^2 + 2bxy + cy^2 = \left(x - \frac{h-b}{a}y\right)\{ax + (h+b)y\}.$$

Wird nun, wie oben in § 127, die Proportion

$$h - b : a = c : -(h + b)$$

aufgestellt und das Verhältniss $h - b : a$, in den kleinsten Zahlen ausgedrückt, $= \beta : \delta$ gesetzt, so geht unsere Zerlegung über in

$$\left(x - \frac{\beta}{\delta} y\right)\left(ax - \frac{c\delta}{\beta} y\right) = (\delta x - \beta y)\left(\frac{a}{\delta} x - \frac{c}{\beta} y\right),$$

so dass sich endlich, wenn

$$\frac{a}{\delta} = f, \qquad \frac{c}{\beta} = g$$

gesetzt wird, wo f, g ganze Zahlen sein werden,

$$ax^2 + 2bxy + cy^2 = (\delta x - \beta y)(fx - gy)$$

ergiebt.

Jede Darstellung von M durch die vorgelegte Form liefert also eine Zerlegung von M in zwei Factoren. Bezeichnen umgekehrt d_1, d_2, d_3 . . . alle Divisoren von M (1 und M nicht ausgeschlossen und jeden sowohl positiv, als negativ genommen), so wird man offenbar alle Darstellungen von M durch die Form (a, b, c) erhalten, wenn man der Reihe nach

$$\begin{cases} \delta x - \beta y = d_1 & \Big| = d_2 & \Big| = \ldots \\ fx - gy = \dfrac{M}{d_1} & \Big| = \dfrac{M}{d_2} & \Big| = \ldots \end{cases}$$

setzt und für jedes dieser Gleichungspaare die Werthe von x und y berechnet. Lösungen in Brüchen sind natürlich zu verwerfen.

Das k^{te} Gleichungspaar liefert

$$x = \frac{d_k^2 g - \beta M}{d_k(\delta g - \beta f)}, \quad y = \frac{d_k^2 f - \delta M}{d_k(\delta g - \beta f)},$$

und da

$$\delta g - \beta f = \frac{\delta c}{\beta} - \frac{\beta a}{\delta} = -(h + b) - (h - b) = -2h,$$

also von Null verschieden ist, so sind die für x, y erhaltenen Werthe völlig bestimmte.

Beispiel. Wir wollen diese Methode auf die oben behandelte Gleichung

$$8x^2 + 26xy + 11y^2 = 585$$

anwenden. Man erhält leicht

$$8x^2 + 26xy + 11y^2 = (2x + y)(4x + 11y),$$

und 585 hat die 24 Divisoren

(± 1), ± 3, (± 5), (± 9), (± 13), ± 15, ± 39, (± 45), (± 65), (± 117), ± 195, (± 585).

Die in Klammern ( ) gesetzten Divisoren würden Lösungen in Brüchen liefern. Wir haben also nur die 8 Gleichungspaare

$$\begin{array}{ll|l|ll} 2x + y & = \pm\ 3 & \pm 15 & \pm 39 & \pm 195 \\ 4x + 11y & = \pm\ 195 & \pm 39 & \pm 15 & \pm\ 3 \end{array}$$

zu lösen, welche die 8 Darstellungen

$$\begin{array}{r|r|r|r|r} x = & \mp\ 9 & \pm 7 & \pm 23 & \pm 119 \\ \hline y = & \pm 21 & \pm 1 & \mp\ 7 & \mp\ 43 \end{array}$$

liefern.

Diese Methode verliert ihre Anwendbarkeit, wenn die darzustellende Zahl $M = 0$, wenn also die Gleichung

$$(\delta x - \beta y)(fx - gy) = 0$$

in ganzen Zahlen zu lösen ist. Die Werthe von x, y müssen dann entweder der Gleichung $\delta x - \beta y = 0$, oder der Gleichung $fx - gx = 0$ genügen. Was nun die erstere betrifft, so sind β, δ prim zu einander; dieselbe hat also die Lösungen

$$(1) \qquad x = \beta k, \qquad y = \delta k,$$

wo k jede (positive oder negative) ganze Zahl sein kann.

Wenn ferner m den grössten gemeinschaftlichen Divisor von f und g bezeichnet, so hat die zweite Gleichung die Lösungen

$$(2) \qquad x = \frac{g}{m} k, \qquad y = \frac{f}{m} k,$$

wo k gleichfalls jede ganze Zahl sein kann. Die Formeln (1) und (2) enthalten alle Lösungen der vorgelegten Aufgabe.

Beispiel. Die Gleichung

$$8x^2 + 30xy + 13y^2 = (2x + y)(4x + 13y) = 0$$

hat die Lösungen

$$\begin{cases} x = k \\ y = -2k \end{cases} \quad \text{und} \quad \begin{cases} x = 13k \\ y = -4k, \end{cases}$$

wo k jede ganze Zahl sein kann.

§ 132. Darstellung der Zahlen durch Formen der Determinante 0. — Es sei die Determinante der Form

(a, b, c) gleich Null, also $b^2 = ac$. Ferner sei m der grösste gemeinschaftliche Divisor von a und c und zwar $a = m\alpha$, $c = m\gamma$, wo also α und γ prim zu einander sind. Da nun $b^2 = m^2\alpha\gamma$ ist, so muss $\alpha\gamma$ eine Quadratzahl sein. Es ist aber α prim zu γ, also muss sowohl α, als auch γ eine Quadratzahl sein.

Dies vorausgesetzt ist

$$ax^2 + 2bxy + cy^2 = m\alpha x^2 + 2m\sqrt{\alpha\gamma}xy + m\gamma y^2$$
$$= m(x\sqrt{\alpha} + y\sqrt{\gamma})^2,$$

und darin ist m der grösste gemeinschaftliche Divisor von a und c, während $\sqrt{\alpha}$, $\sqrt{\gamma}$ ganze Zahlen sind.

Soll nun M durch die Form (a, b, c) dargestellt werden können, so muss M durch m theilbar und der Quotient eine Quadratzahl sein. Wird dieser Quotient mit q^2 bezeichnet, so ist

$$x\sqrt{\alpha} + y\sqrt{\gamma} = +q \quad \text{und} \quad = -q$$

zu setzen, und es ergeben sich alle Darstellungen von M, indem man alle ganzzahligen Lösungen dieser beiden unbestimmten Gleichungen ersten Grades ermittelt, welche, da $\sqrt{\alpha}$ prim zu $\sqrt{\gamma}$ ist, stets lösbar sind.

Beispiel. Die Gleichung

$$12x^2 + 36xy + 27y^2 = 75$$

ist in ganzen Zahlen lösbar, da der grösste gemeinschaftliche Divisor 3 der Zahlen 12, 27 (dessen Quadrat in $b = 18$ aufgeht) in 75 aufgeht und als Quotienten eine Quadratzahl, nämlich 25, liefert. Durch Division mit 3 erhält man

$$4x^2 + 12xy + 9y^2 = (2x + 3y)^2 = 25;$$

es ist also

$$2x + 3y = +5 \quad \text{und} \quad = -5$$

zu setzen. Die Lösungen dieser beiden Gleichungen

$$\begin{cases} x = 1 + 3k \\ y = 1 - 2k \end{cases}, \qquad \begin{cases} x = -1 - 3k \\ y = -1 + 2k \end{cases},$$

in denen k jede ganze Zahl sein kann, enthalten alle Darstellungen von 75 durch die Form (12, 18, 27).

§ 133. Auflösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten. — Wir sind jetzt im Stande, die allgemeine Gleichung zweiten Grades mit zwei Unbekannten, der wir immer die Form

$$(1) \qquad ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

geben können, in ganzen Zahlen aufzulösen.

Wir setzen

$$x = \xi + \alpha, \quad y = \eta + \beta;$$

dann geht (1) über in

$$a\xi^2 + 2b\xi\eta + c\eta^2 + 2\xi(a\alpha + b\beta + d) + 2\eta(b\alpha + c\beta + e) + (a\alpha^2 + 2b\alpha\beta + c\beta^2 + 2d\alpha + 2e\beta + f) = 0.$$

Verfügen wir jetzt über die noch unbestimmten Grössen α, β in der Weise, dass

$$a\alpha + b\beta + d = 0,$$
$$b\alpha + c\beta + e = 0$$

wird, nehmen also

$$\alpha = \frac{cd - be}{b^2 - ac}, \quad \beta = \frac{ae - bd}{b^2 - ac}$$

an, so erhalten wir statt der Gleichung (1)

$$(2) \quad a\xi^2 + 2b\xi\eta + c\eta^2 + \frac{(b^2 - ac)(ae^2 - 2bde + cd^2) + f(b^2 - ac)^2}{(b^2 - ac)^2} = 0$$

oder, wenn wir beiderseits mit $(b^2 - ac)^2$ multipliciren und der Kürze wegen

$$\xi(b^2 - ac) = X, \; \eta(b^2 - ac) = Y,$$

$$(b^2 - ac)(ae^2 - 2bde + cd^2) + f(b^2 - ac)^2 = -M$$

setzen,

$$(3) \qquad aX^2 + 2bXY + cY^2 = M.$$

Die Gleichung (3) in ganzen Zahlen aufzulösen, ist oben für alle Fälle, die sich darbieten können, gelehrt worden.

Hat man X, Y bestimmt, so liefern die Formeln

$$(4) \qquad x = \frac{X + cd - be}{b^2 - ac}, \quad y = \frac{Y + ae - bd}{b^2 - ac}$$

die entsprechenden Werthe von x, y.

Wie man sofort sieht, sind X, Y ganze Zahlen, sobald x, y ganze Zahlen sind; daher wird jede Lösung von (1) in

ganzen Zahlen auch durch die Formeln (4) geliefert werden. Dagegen können diese Formeln auch gebrochene Werthe für x, y geben, die dann natürlich zu verwerfen sind.

1. **Beispiel.** Es soll die Gleichung

$$3x^2 + 4xy + 2y^2 - 2x + 10y - 28 = 0$$

in ganzen Zahlen aufgelöst werden. Die oben dargelegte Substitution führt zu der neuen Gleichung

$$3X^2 + 4XY + 2Y^2 = 306.$$

Die Determinante der Form (3, 2, 2) ist -2. Wir lösen also zunächst die Congruenz

$$\xi^2 \equiv -2 \pmod{306 = 2 \cdot 3^2 \cdot 17};$$

dieselbe hat die 4 Wurzeln ± 58, ± 112, die wir einzeln zu prüfen haben.

1. Darstellungen, die zur Wurzel $+58$ gehören.

Reihe der benachbarten Formen:

(3, 2, 2), (2, 0, 1), (1, 3, 11), (11, -58, 306), (306, 58, 11).

$h_1 = 1$	$h_2 = 3$	$h_3 = -5$	$h_4 = 0$	
0	-1	-3	16	3
1	1	2	-11	-2

Da $m = 1$, also $\frac{4|D|}{m^2} > 4$ ist, so ergeben sich nur die beiden Darstellungen:

$$X = \pm 16, \quad Y = \mp 11.$$

2. Darstellungen, die zu -58 gehören.

Formenreihe:

(3, 2, 2), (2, 0, 1), (1, -3, 11), (11, 58, 306), (306, -58, 11).

$h_1 = 1$	$h_2 = -3$	$h_3 = 5$	$h_4 = 0$	
0	-1	3	16	-3
1	1	-4	21	4

Darstellungen: $X = \pm 16$, $Y = \mp 21$.

3. Darstellungen, die zu $+112$ gehören.

Formenreihe:

$$(3,\ 2,\ 2),\ (2,\ 0,\ 1),\ (1,\ -1,\ 3),\ (3,\ -11,\ 41),\ (41,\ -112,\ 306),\ (306,\ 112,\ 41).$$

$h_1 = 1$	$h_2 = -1$	$h_3 = -4$	$h_4 = -3$	$h_5 = 0$	
0	-1	1	-3	-8	3
1	1	-2	7	-19	-7

Darstellungen: $X = \pm 8,\ Y = \mp 19$.

4. Darstellungen, die zu -112 gehören.

Formenreihe:

$$(3,\ 2,\ 2),\ (2,\ 0,\ 1),\ (1,\ 1,\ 3),\ (3,\ 11,\ 41),\ (41,\ 112,\ 306),\ (306,\ -112,\ 41).$$

$h_1 = 1$	$h_2 = 1$	$h_3 = 4$	$h_4 = 3$	$h_5 = 0$	
0	-1	-1	-3	-8	3
1	1	0	-1	-3	1

Darstellungen: $X = \pm 8,\ Y = \pm 3$.

5. Uneigentliche Darstellungen. Setzen wir

$$X = 3X',\ Y = 3Y',$$

so erhalten wir, indem wir den Factor 9 beiderseits fortlassen,

$$3X'^2 + 4X'Y'^2 + 2Y'^2 = 34.$$

Die Congruenz

$$\xi^2 \equiv -2 \pmod{34}$$

hat die beiden Wurzeln ± 10.

Der ersten Wurzel entspricht die Formenreihe

$$(3,\ 2,\ 2),\ (2,\ 0,\ 1),\ (1,\ 1,\ 3),\ (3,\ -10,\ 34),\ (34,\ 10,\ 3).$$

$h_1 = 1$	$h_2 = 1$	$h_3 = -3$	$h_4 = 0$	
0	-1	-1	4	1
1	1	0	-1	0

Darstellungen: $X' = \pm 4,\ Y' = \mp 1$,

also $X = \pm 12,\ Y = \mp 3$.

Der zweiten Wurzel entspricht die Formenreihe

$(3, 2, 2), (2, 0, 1), (1, -1, 3), (3, 10, 34), (34, -10, 3).$

$h_1 = 1$	$h_2 = -1$	$h_3 = 3$	$h_4 = 0$	
0	-1	1	4	-1
1	1	-2	-7	2

Darstellungen: $X' = \pm 4$, $Y' = \mp 7$,
also

$$X = \pm 12, \quad Y = \mp 21.$$

Nachdem wir so X, Y bestimmt haben, liefern die Formeln (4), die für die vorliegende Gleichung in

$$x = \frac{X - 12}{-2}, \quad y = \frac{Y + 17}{2}$$

übergehen, die entsprechenden Werthe von x, y. Man erhält die 12 Lösungen:

x	-2	14	-2	14	2	10	2	10
y	-3	-14	$+2$	-19	1	-18	-10	-7

x	0	12	0	12
y	-7	-10	2	-19

2. Beispiel. Die Gleichung

$$x^2 + 2xy - 5y^2 + 4x - 10y \quad 13 = 0$$

geht über in

$$X^2 + 2XY - 5Y^2 = 318,$$

wo

$$x = \frac{X - 5}{6}, \quad y = \frac{Y - 7}{6}$$

ist. Zunächst haben wir die Hülfsgleichung

$$t^2 - 6u^2 = 1$$

zu lösen.

$$(1, 2, -2), (-2, 2, 1), (1, 2, -2).$$

2	4	
1	2	9
0	1	4

also $$\alpha = 1,\ \beta = 4,\ \gamma = 2,\ \delta = 9,$$
$$T = 5,\ U = 2,\ \frac{2T}{m} = 10$$
und

t	1	5	$10 \cdot 5 - 1 = 49$	$10 \cdot 49 - 5 = 485$	$\cdots$
u	0	2	$10 \cdot 2 - 0 = 20$	$10 \cdot 20 - 2 = 198$	$\cdots$,

wo jede Colonne 4 Lösungen darstellt.

Nun hat die Congruenz
$$\xi^2 \equiv 6 \pmod{318}$$
die beiden Wurzeln ± 18.

1. Darstellungen, die zu $+18$ gehören.

Formenreihe:
$$(1, 1, -5),\ (-5, -1, 1),\ (1, -18, 318),\ (318, 18, 1).$$

0	-19	0	
0	-1	19	1
1	0	-1	0

Darstellungen: $X = 19t - 24u$, $Y = -t + 18u$,

also
$$\begin{cases} x = \dfrac{19t - 24u - 5}{6} = 3t - 4u - 1 + \dfrac{t+1}{6} \\ y = \dfrac{-t + 18u - 7}{6} = 3u - 1 - \dfrac{t+1}{6}. \end{cases}$$

Ganze Werthe von x, y liefern also nur diejenigen Lösungen der Pell'schen Gleichung, bei denen $t + 1$ durch 6 theilbar ist, also z. B.

t	-1	$+5$	$+5$	-49	-49	$\cdots$
u	0	$+2$	-2	$+20$	-20	$\cdots$
x	-4	$+7$	$+23$	-236	-76	$\cdots$
y	-1	$+4$	-8	$+67$	-53	$\cdots$

2. Darstellungen, die zu -18 gehören.

Formenreihe:
$$(1, 1, -5),\ (-5, -1, 1),\ (1, 18, 318),\ (318, -18, 1).$$

0	17	0	
0	-1	-17	1
1	0	-1	0

Darstellungen: $\begin{cases} X = -17t + 12u \\ Y = -t - 18u, \end{cases}$

also

$$\begin{cases} x = \dfrac{-17t + 12u - 5}{6} = -3t + 2u - 1 + \dfrac{t+1}{6} \\ y = \dfrac{-t - 18u - 7}{6} = -3u - 1 - \dfrac{t+1}{6}. \end{cases}$$

Hinsichtlich der ganzen Werthe von x, y gilt dieselbe Bemerkung wie oben. Man erhält z. B. die Tabelle

t	-1	$+5$	$+5$	-49	-49	...
u	0	$+2$	-2	$+20$	-20	...
x	$+2$	-19	-11	$+178$	$+98$	...
y	-1	-8	$+4$	-53	$+67$	... .

INDEX-TAFELN.

I.

Modul	Pr. Wrzl.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		Index der Zahl																								
3	2	2	1																							
4	3	2	—	1																						
5	2	4	1	3	2																					
6	5	2	—	—	—	1																				
7	3	6	2	1	4	5	3																			
8	3	2	—	1	—		—																			
9	2	6	1	—	2	5		4	3																	
10	3	4	—	1	—	—	—	3	—	2																
11	2	10	1	8	2	4	9	7	3	6	5															
13	2	12	1	4	2	9	5	11	3	8	10	7	6													
14	3	6	—	1	—	5	—	—	—	2	—	4		3												
16	3	4		1	—		—		—	2		3	—		—											
17	3	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8									
18	5	6		—	—	1	—	2	—		—	5		4	—	·	—	3								
19	2	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9							
22	7	10	—	4	—	2	—	1	—	8		—		3	—	6		7		9	—	5				
23	5	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11			
25	2	20	1	7	2	—	8	5	3	14		16	9	19	6	—	4	13	15	18	—	12	17	11	10	
26	7	12	—	8	—	3	—	1	—	1	—	5	—	—		11	—	10	—	7	—	9		2	—	6

Modul	Pr. Wrzl.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		Index der Zahl																								
27	2	18	1	—	2	5	—	16	3		6	13		8	17		4	15		12	7		14	11	-	10
29	2	28	1	5	2	22	6	12	3	10	23	25	7	18	13	27	4	21	11	9	24	17	26	20	8	16
31	3	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21	6	7	26	4	8	29	17	27	13	10
32	3	8	—	1	—		—		—	2		7	—		—		—	4	—	5			—		—	6
34	3	16	—	1		5	—	11	—	2		7	—	4	—	6	—	—	—	14		12	—	15	—	10
37	2	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17	35	25	22	31	15	29	10
38	3	18	—	1	—	4	—	6	—	2		12	—	17	—	5	—	16	—		—	7	—	14	—	8
41	6	40	26	15	12	22	1	39	38	30	8	3	27	31	25	37	24	33	16	9	34	14	29	36	13	4
43	3	42	27	1	12	25	28	35	39	2	10	30	13	32	20	26	24	38	29	19	37	36	15	16	40	8
46	5	22	—	16	—	1		19	—	10	—	9	—	14	—	17	-	7		15		13				2
47	5	46	18	20	36	1	38	32	8	40	19	7	10	11	4	21	26	16	12	45	37	6	25	5	28	2
49	3	42	26	1	10	29	27		36	2	13	40	11	33	—	30	20	25	28	35	39	—	24	38	37	16
50	3	20	—	1	—	—		15	—	2		8		17	—		-	19		14		16	—	13		—

Modul	Pr. Wrzl.	Index der Zahl 26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
27	2	9																							
29	2	19	15	14																					
31	3	5	3	16	9	15																			
32	3	—	3	—		—																			
34	3	—	3	—	13	—	9	—	8																
37	2	12	6	34	21	14	9	5	20	8	19	18													
38	3	—	3	—	11	—	15	—	13	—	10	—	9												
41	6	17	5	11	7	23	28	10	18	19	21	2	32	35	6	20									
43	3	17	3	5	41	11	34	9	31	23	18	14	7	4	33	22	6	21							
46	5	—	4	—	18	—	6	—	3	—	20	—	21	—	8	—	12	—	5	—	11				
47	5	29	14	22	35	39	3	44	27	34	33	30	42	17	31	9	15	24	13	43	41	23			
49	3	17	3	—	18	14	7	4	41	9	—	12	32	19	34	23	15	—	6	8	31	22	5	21	
50	3	—	3	—	6	—	4	—	9	—	—	—	7	—	18	—	12	—	5	—	—	—	11	—	10

Modul	Pr. Wrzl.	Index der Zahl 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
53	2	52	1	17	2	47	18	14	3	34	48	6	19	24	15	12	4	10	35	37	49	31	7	39	20	42
54	5	18	—	—	—	1	—	14	—	—	—	17	—	16	—	—	—	3	—	6	—	—	—	13	—	2
58	3	28	—	1	—	10	—	8	—	2	—	5	—	26	—	11	—	21	—	13	—	9	—	4	—	20
59	2	58	1	50	2	6	51	18	3	42	7	25	52	45	19	56	4	40	43	38	8	10	26	15	53	12
61	2	60	1	6	2	22	7	49	3	12	23	15	8	40	50	28	4	47	13	26	24	55	16	57	9	44
62	3	30	—	1	—	20	—	28	—	2	—	23	—	11	—	21	—	7	—	4	—	29	—	27	—	10
64	3	16	—	1	—		—		—	2	—	7	—		—		—	4	—	13	—		—		—	6
67	2	66	1	39	2	15	40	23	3	12	16	59	41	19	24	54	4	64	13	10	17	62	60	28	42	30
71	7	70	6	26	12	28	32	1	18	52	34	31	38	39	7	54	24	49	58	16	40	27	37	15	44	56
73	5	72	8	6	16	1	11	33	24	12	9	55	22	59	41	7	32	21	20	62	17	39	63	46	30	2
74	5	36	—	34	—	1	—	28	—	32	—	6	—	13	—	35	—	5	—	25	—	26	—	21	—	2

Modul	Pr. Wrzl.	Index der Zahl 26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
53	2	25	51	16	46	13	33	5	23	11	9	36	30	38	41	50	45	32	22	8	29	40	44	21	28	43
54	5	—	—	—	11	—	4	—	—	—	15	—	12	—	—	—	7	—	8	—	—	—	5	—	10	—
58	3	—	3	—	—	—	17	—	6	—	18		23	—	27	—	7	—	25	—	12	—	19	—	16	—
59	2	46	34	20	28	57	49	5	17	41	24	44	55	39	37	9	14	11	33	27	48	16	23	54	36	13
61	2	41	18	51	35	29	59	5	21	48	11	14	39	27	46	25	54	56	43	17	34	58	20	10	38	45
62	3	—	3	—	9		—		24	—	18		25	—	12	—	14		19	—	22	—	6	—	26	—
64	3	—	3	—		—		—	8	—	9	—		—		—	10	—	15	—		—		—	12	—
67	2	20	51	25	44	55	47	5	32	65	38	14	22	11	58	18	53	63	9	61	27	29	50	43	46	31
71	7	15	8	13	68	60	11	30	57	55	29	64	20	22	65	46	25	33	48	43	10	21	9	50	2	62
73	5	67	18	49	35	15	11	40	61	29	34	28	64	70	65	25	4	47	51	71	13	54	31	38	66	10
74	5	—	30	—	15	—	27	—	4	—	29		—	—	11	—	22	—	9	—	33	—	12		20	—

Modul	Pr. Wrzl.	Index der Zahl																								
		51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
53	2	27	26																							
54	5	—	—	9	—																					
58	3	22	—	24	—	15	—	14																		
59	2	32	47	22	35	31	21	30	29																	
61	2	53	42	33	19	37	52	32	36	31	30															
62	3	8	—	17	—	13	—	5	—	16	—	15														
64	3	5	—		—		—	14	—	11	—		—													
67	2	37	21	57	52	8	26	49	45	36	56	7	48	35	6	34	33									
71	7	5	51	23	14	59	19	42	4	3	66	69	17	53	36	67	63	47	61	41	35					
73	5	27	3	53	26	56	57	68	43	5	23	58	19	45	48	60	69	50	37	52	42	44	36			
74	5	3	—	8	—	7	—	23	—	17	—	31	—	24	—	14	—	10	—	19	—	16	—	18		

Modul	Pr. Wrzl.	Index der Zahl																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
79	3	78	4	1	8	62	5	53	12	2	66	68	9	34	57	63	16	21	6	32	70	54	72	26	13	46
81	2	54	1	—	2	23	—	16	3	—	24	13	—	8	17		4	33	—	48	25	—	14	11	—	46
82	7	40	—	25	—	18	—	1	—	10	—	37	—	9	—	3	—	7	—	31	—	26	—	4	—	36
83	2	82	1	72	2	27	73	8	3	62	28	24	74	77	9	17	4	56	63	47	29	80	25	60	75	54
86	3	42	—	1	—	25	—	35	—	2	—	30	—	32	—	26	—	38	—	19	—	36	—	16	—	8
89	3	88	16	1	32	70	17	81	48	2	86	84	33	23	9	71	64	6	18	35	14	82	12	57	49	52
94	5	46	—	20	—	1	—	32	—	40	—	7	—	11	—	21	—	16	—	45		6	—	5	—	2
97	5	96	34	70	68	1	8	31	6	44	35	86	42	25	65	71	40	89	78	81	69	5	24	77	76	2
98	3	42	—	1	—	29	—	—	—	2	—	40	—	33	—	30	—	25	—	35	—	—	—	38	—	16

Modul	Pr. Wrzl.	Index der Zahl																								
		26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
79	3	38	3	61	11	67	56	20	69	25	37	10	19	36	35	74	75	58	49	76	64	30	59	17	28	50
81	2	9	—	18	37	—	20	5	—	34	39	—	42	49	—	26	53	—	22	15		12	7	—	32	47
82	7	—	35	—	33	—	12		22	—	19	—	8	—	34	—	—	—	14	—	28	—	39	—	2	—
83	2	78	52	10	12	18	38	5	14	57	35	64	20	48	67	30	40	81	71	26	7	61	23	76	16	55
86	3	—	3	—	41	—	34	—	31	—	18	—	7	—	33	—	6	—	—	—	27	—	12	—	28	—
89	3	39	3	25	59	87	31	80	85	22	63	34	11	51	24	30	21	10	29	28	72	73	54	65	74	68
94	5	—	14	—	35	—	3	—	27	—	33	—	42	—	31	—	15	—	13	—	41	—	—	—	18	—
97	5	59	18	3	13	9	46	74	60	27	32	16	91	19	95	7	85	39	4	58	45	15	84	14	62	36
98	3	—	3	—	18	—	7	—	41	—	—	—	32	—	34	—	15		6	—	31	—	5		—	—

Modul	Pr. Wrzl.	Index der Zahl																								
		51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
79	3	22	42	77	7	52	65	33	15	31	71	45	60	55	24	18	73	48	29	27	41	51	14	44	23	47
81	2	—	10	45	—	36	19	—	38	41	—	52	21	—	6	31	—	44	35	—	40	51	—	30	43	—
82	7	32	—	13	—	15	—	16	—	24	—	6	—	11	—	27	—	23	—	29	—	17		30	—	21
83	2	46	79	59	53	51	11	37	13	34	19	66	39	70	6	22	15	45	58	50	36	33	65	69	21	44
86	3	39	—	10	—	13	—	20	—	24	—	29	—	37	—	15	—	40	—	17	—	5	—	11	—	9
89	3	7	55	78	19	66	41	36	75	43	15	69	47	83	8	5	13	56	38	58	79	62	50	20	27	53
94	5	36	—	38	—	8	—	19	—	10	—	4	—	26	—	12	—	37	—	25	—	28	—	29	—	22
97	5	63	93	10	52	87	37	55	47	67	13	64	80	75	12	26	94	57	61	51	66	11	50	28	29	72
98	3	26	—	10	—	27	—	36	—	13	—	11	—	—	—	20	—	28	—	39	—	24	—	37	—	17

Modul	Pr. W.	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
		Index der Zahl																								
79	3	40	43	39																						
81	2	50	29	—	28	27																				
82	7	—	38	—	5		20																			
83	2	49	32	68	43	31	42	41																		
86	3		23	—	14	—	4	—	22	—	21															
89	3	67	77	40	42	46	4	37	61	26	76	45	60	44												
94	5	—	39	—	44	—	31	—	30	—	17	—	9	—	24	—	43	—	23							
97	5	53	21	33	30	41	88	23	17	73	90	38	83	92	54	79	56	49	20	22	82	48				
98	3	—	—	—	14	—	4	—	9	—	12	—	19	—	23	—	—	—	8	—	22	—	21			

II.

Modul	Pr. W.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		Zahl, gehörend zu dem Index																								
3	2	2	1																							
4	3	3	1																							
5	2	2	4	3	1																					
6	5	5	1																							
7	3	3	2	6	4	5	1																			
8	3	3	1																							
9	2	2	4	8	7	5	1																			
10	3	3	9	7	1																					
11	2	2	4	8	5	10	9	7	3	6	1															
13	2	2	4	8	3	6	12	11	9	5	10	7	1													
14	3	3	9	13	11	5	1																			
16	3	3	9	11	1																					
17	3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1									
18	5	5	7	17	13	11	1																			
19	2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1							
22	7	7	5	13	3	21	15	17	9	19	1															
23	5	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1			
25	2	2	4	8	16	7	11	3	6	12	24	23	21	17	9	18	11	22	19	13	1					
26	7	7	23	5	9	11	25	19	3	21	17	15	1													

Modul	Pr. W.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		Zahl, gehörend zu dem Index																								
27	2	2	4	8	16	5	10	20	13	26	25	23	19	11	22	17	7	14	1							
29	2	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25	21	13	26	23	17	5	10	20	11
31	3	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28	22	4	12	5	15	14	11	2	6
32	3	3	9	27	17	19	25	11	1																	
34	3	3	9	27	13	5	15	11	33	31	25	7	21	29	19	23	1									
37	2	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36	35	33	29	21	5	10	20
38	3	3	9	27	5	15	7	21	25	37	35	29	11	33	23	31	17	13	1							
41	6	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	40	35	5	30	16	14
43	3	3	9	27	38	28	11	37	25	32	10	30	4	12	36	22	23	26	35	19	14	42	40	34	16	5
46	5	5	25	33	27	43	31	17	39	11	9	45	41	21	13	19	3	15	29	7	35	37	1			
47	5	5	25	31	14	23	21	11	8	40	12	13	18	43	27	41	17	38	2	10	3	15	28	46	42	22
49	3	3	9	27	32	47	43	31	44	34	4	12	36	10	30	11	25	26	29	38	16	48	46	10	22	17
50	3	3	9	27	31	43	29	37	11	33	49	47	41	23	19	7	21	13	39	17	1					

Modul	Pr. Wrzl.	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
		Zahl, gehörend zu dem Index																								
27	2																									
29	2	22	15	1																						
31	3	18	23	7	21	1																				
32	3																									
34	3																									
37	2	3	6	12	24	11	22	7	14	28	19	1														
38	3																									
41	6	2	12	31	22	9	13	37	17	20	38	23	15	8	7	1										
43	3	15	2	6	18	11	33	13	39	31	7	21	20	17	8	24	29	1								
46	5																									
47	5	16	33	24	26	36	39	7	35	34	29	4	20	6	30	9	45	37	44	32	19	1				
49	3	2	6	18	5	15	45	37	13	39	19	8	24	23	20	11	33	1								
50	3																									

Modul	Pr. Wrzl.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		Zahl, gehörend zu dem Index																								
53	2	2	4	8	16	32	11	22	44	35	17	34	15	30	7	14	28	3	6	12	24	48	43	33	13	26
54	5	5	25	17	31	47	19	41	43	53	49	29	37	23	7	35	13	11	1							
58	3	3	9	27	23	11	33	41	7	21	5	15	45	19	57	55	49	31	35	47	25	17	51	37	53	43
59	2	2	4	8	16	32	5	10	20	40	21	42	25	50	41	23	46	33	7	14	28	56	53	47	35	11
61	2	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11	22	44	27	54	47	33	5	10	20	40
62	3	3	9	27	19	57	47	17	51	29	25	13	39	55	41	61	59	53	35	43	5	15	45	11	33	37
64	3	3	9	27	17	51	25	11	33	35	41	59	49	19	57	43	1									
67	2	2	4	8	16	32	64	61	55	43	19	38	9	18	36	5	10	20	40	13	26	52	37	7	14	28
71	7	7	49	59	58	51	2	14	27	47	45	31	4	28	54	23	19	62	8	56	37	46	38	53	16	41
73	5	5	25	52	41	59	3	15	2	10	50	31	9	45	6	30	4	20	27	62	18	17	12	60	8	40
74	5	5	25	51	33	17	11	55	53	43	67	39	47	13	65	29	71	59	73	69	49	23	41	57	63	19

Modul	Pr. Wrzl.	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
		Zahl, gehörend zu dem Index																								
53	2	52	51	49	45	37	21	42	31	9	18	36	19	38	23	46	39	25	50	47	41	29	5	10	20	40
54	5																									
58	3	13	39	1																						
59	2	22	44	29	58	57	55	51	43	27	54	49	39	19	38	17	34	9	18	36	13	26	52	45	31	3
61	2	19	38	15	30	60	59	57	53	45	29	58	55	49	37	13	26	52	43	25	50	39	17	34	7	14
62	3	49	23	7	21	1																				
64	3																									
67	2	56	45	23	46	25	50	33	66	65	63	59	51	35	3	6	12	24	48	29	58	49	31	62	57	47
71	7	3	21	5	35	32	11	6	42	10	70	64	22	12	13	20	69	57	44	24	26	40	67	43	17	48
73	5	54	51	36	34	21	47	16	7	35	29	72	68	48	21	32	14	70	58	71	63	23	42	64	28	67
74	5	21	31	7	35	27	61	9	45	3	15	1														

Modul	Pr. Wurzel	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
		Zahl, gehörend zu dem Index																								
53	2	27	1																							
54	5																									
58	3																									
59	2	6	12	24	48	37	15	30	1																	
61	2	28	56	51	41	21	42	23	46	31	1															
62	3																									
64	3																									
67	2	27	54	41	15	30	60	53	39	11	22	44	21	42	17	34	1									
71	7	52	9	63	15	34	25	33	18	55	30	68	50	66	36	39	60	65	29	61	1					
73	5	43	69	53	46	11	55	56	61	13	65	33	19	22	37	39	49	26	57	66	38	44	1			
74	5																									

Modul	Pr. Wurzel	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		Zahl, gehörend zu dem Index																								
79	3	3	9	27	2	6	18	54	4	12	36	29	8	24	72	58	16	48	65	37	32	17	51	74	64	34
81	2	2	4	8	16	32	64	47	13	26	52	23	46	11	22	44	7	14	28	56	31	62	43	5	10	20
82	7	7	49	15	23	79	61	17	37	13	9	63	31	53	43	55	57	71	5	35	81	75	33	67	59	3
83	2	2	4	8	16	32	64	45	7	14	28	56	29	58	33	66	49	15	30	60	37	74	65	47	11	22
86	3	3	9	27	81	71	41	37	25	75	53	73	47	55	79	65	23	69	35	19	57	85	83	77	59	5
89	3	3	9	27	81	65	17	51	64	14	42	37	22	66	20	60	2	6	18	54	73	41	34	13	39	28
94	5	5	25	31	61	23	21	11	55	87	59	13	65	43	27	41	17	85	49	57	3	15	75	93	89	69
97	5	5	25	28	43	21	8	40	6	30	53	71	64	29	48	46	36	83	27	38	93	77	94	82	22	13
98	3	3	9	27	81	47	43	31	93	83	53	61	85	59	79	41	25	75	29	87	65	97	95	89	71	17

Modul	Pr. Wurzel	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
		Zahl, gehörend zu dem Index																								
79	3	23	69	49	68	46	59	19	57	13	39	38	35	26	78	76	70	52	77	73	61	25	75	67	43	50
81	2	40	80	79	77	73	65	49	17	34	68	55	29	58	35	70	59	37	74	67	53	25	50	19	38	76
82	7	21	65	15	69	73	19	51	29	39	27	25	11	77	47	1										
83	2	44	5	10	20	40	80	77	71	59	35	70	57	31	62	41	82	81	79	75	67	51	19	38	76	69
86	3	15	45	49	61	11	33	13	39	31	7	21	63	17	51	67	29	1								
89	3	84	74	44	43	40	31	4	12	36	19	57	82	68	26	78	56	79	59	88	86	80	62	8	24	72
94	5	63	33	71	73	83	39	7	35	81	29	51	67	53	77	9	45	37	91	79	19	1				
97	5	65	34	73	74	79	7	35	78	2	10	50	56	86	42	16	80	12	60	9	45	31	58	96	92	72
98	3	51	55	67	5	15	45	37	13	39	19	57	73	23	69	11	33	1								

Modul	Pr. Wurzel	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
		Zahl, gehörend zu dem Index																								
79	3	71	55	7	21	63	31	14	42	47	62	28	5	15	45	56	10	30	11	33	20	60	22	66	40	41
81	2	71	61	41	1																					
82	7																									
83	2	55	27	54	25	50	17	34	68	53	23	46	9	18	36	72	61	39	78	73	63	43	3	6	12	24
86	3																									
89	3	38	25	75	47	52	67	23	69	29	87	83	71	35	16	48	55	76	50	61	5	15	45	46	49	58
94	5																									
97	5	69	54	76	89	57	91	67	44	26	33	68	49	51	61	14	70	59	4	20	3	15	75	84	32	63
98	3																									

Modul	Pr. Wrzl	Zahl, gehörend zu dem Index																							
		76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
79	3	44	53	1																						
81	2																									
82	7																									
83	2	48	13	26	52	21	42	1																		
86	3																									
89	3	85	77	53	70	32	7	21	63	11	33	10	30	1												
94	5																									
97	5	24	23	18	90	62	19	95	87	47	41	11	55	81	17	85	37	88	52	66	39		1			
98	3																									

Druckfehler.

Seite 207, Zeile 7 v. o. streiche „zweiten Grades."

VORLESUNGEN

ÜBER DIE

NATUR DER IRRATIONALZAHLEN

VON

PAUL BACHMANN.



LEIPZIG,

DRUCK UND VERLAG VON B. G. TEUBNER.

1892.



Vorrede.

Die irrationalen Zahlen haben stets das Interesse der Mathematiker in hervorragender Weise in Anspruch genommen. Theils mussten diese ihre Bemühungen darauf richten, eine genaue und widerspruchsfreie Fassung des Begriffs derselben zu geben, in welcher ihr eigentliches Wesen zum Ausdruck kommt, und so ihre Einführung in die Rechnung fest zu begründen; theils reizte die unendliche Mannigfaltigkeit der Irrationalzahlen, auf welche Algebra und höhere Analysis führten, zu der Frage, in welcher Weise sie unter einander verbunden und wieder von einander unterschieden sind, und wie eine jede einzelne Gattung derselben in eigenthümlicher Weise zu kennzeichnen, kurz, welches die eigentliche arithmetische Natur der einzelnen Irrationalzahlen sei.

In beiden Beziehungen sind gerade in neuerer Zeit die Irrationalzahlen wieder vorzüglicher Gegenstand der Betrachtung geworden. Die feinere Ausbildung des Funktionsbegriffes und anderer damit zusammenhangender fundamentaler Punkte der Differenzial- und Integral-Rechnung auf der einen, die strengere Begründung der Lehre von den complexen Grössen und ihrer Funktionen auf der anderen Seite sind Anlass geworden, dass die Mathematiker der Neuzeit wie auf den Zahlenbegriff überhaupt, so insbesondere auch auf eine angemessene Definition der Irrationalzahlen mit Vorliebe wieder ihre Aufmerksamkeit gerichtet haben. Vor allen war es hier Herr Weierstrass, der in seinen Vorlesungen über Funktionentheorie in systematischer Weise sich darüber verbreitete; von seinen Gedanken hat einer seiner Schüler, Herr Kossak

(im Programm des Friedrich-Werder'schen Gymnasiums zu Berlin, 1872) eine ausführliche Darstellung gegeben. Nach ihm seien hier nur erwähnt die Arbeiten von E. Heine (Journal für die r. u. a. Mathematik Bd. 74, pag. 172)*), von Herrn Dedekind (Stetigkeit und irrationale Zahlen, Braunschweig 1872, und: Was sind und was sollen die Zahlen? ebendas. 1888), sowie die Abhandlung von Herrn Kronecker über den Zahlbegriff (im Journal f. d. r. u. a. M. 101. Bd.).

Aber auch in der zweitgenannten Richtung hat die neueste Zeit einige epochemachende Untersuchungen und Ergebnisse zu verzeichnen. Nachdem es bereits Liouville gelungen war, zu beweisen, dass es Irrationellen giebt, welche auf keine Weise als Wurzeln algebraischer Gleichungen aufgefasst werden können, war es in hohem Grade interessant zu entscheiden, ob die überall in der Analysis auftretenden beiden, durch e und π bezeichneten Zahlen zu diesen nicht algebraischen Irrationalzahlen zu rechnen sind. Es ist das Verdienst des Herrn Hermite, auf sehr genialem Wege nachgewiesen zu haben, dass die Zahl e eine transcendente Zahl ist; und weiter bauend auf den von ihm gegebenen Grundlagen erreichte Herr Lindemann den gleichen Nachweis auch für die Ludolph'sche Zahl π, und bewies damit zugleich, dass die Quadratur des Kreises eine Unmöglichkeit sei. Da hiermit die Untersuchungen über die Natur der Irrationalzahlen in einem der interessantesten Punkte zu einem gewissen Abschlusse gelangt sind, hat der Verfasser dieses Buches es für zeitgemäss und erwünscht erachtet, die wichtigsten Untersuchungen, welche bisher in der angegebenen Richtung geführt worden sind, für einen grösseren mathematischen Leserkreis im Zusammenhange darzustellen, indem er eine Vorlesung, die er zu wiederholten Malen über diesen Gegenstand gehalten, weiter ausführte; wobei er, um den Inhalt des Buches möglichst weiten Kreisen zugänglich zu

*) Vgl. dazu G. Cantor's Abh. in Math. Annalen Bd. 5 pag. 123, oder seine Mannigfaltigkeitslehre, Leipz. 1883, pag. 21. Den Standpunkt dieser Arbeiten habe ich im wesentlichen zu dem meinigen gemacht trotz der Kritik, welche die Aufsätze von Illigens, Math. Ann. Bd. 33 u. 35 an ihm üben; die Begründung dafür muss ich für eine andere Stelle mir vorbehalten.

machen, das Mass der Vorkenntnisse thunlichst zu beschränken bemüht gewesen ist.

Nachdem dabei die Irrationalzahlen, im wesentlichen nach Heine's Gesichtspunkten, begrifflich festgestellt sind, wobei eine grössere Anschaulichkeit erreicht sein dürfte durch Einführung des Begriffes „zweier gegen einander convergirender Werthreihen", werden einige Fundamentalsätze von algebraischen Zahlen hergeleitet, welche auf ihre allgemeinste Definition sich beziehen. Nach dem Grade der Gleichung, durch welche sie bestimmt sind, können sie unterschieden werden in quadratische, kubische Irrationellen u. s. w., und es fragt sich, welche rein arithmetischen Kennzeichen dieser algebraischen Eintheilung adäquat sind. Dasjenige für die quadratischen Irrationellen ist seit längerer Zeit schon bekannt und besteht darin, dass sie und nur sie allein in periodische Kettenbrüche entwickelbar sind; für die Irrationellen höheren Grades fehlt jedoch noch jedes ähnliche Kennzeichen, und nur ein erster Schritt, zu einem solchen zu gelangen, darf in einer Arbeit von Jacobi über Kettenbruchalgorithmen erblickt werden. Im Folgenden wird nun zunächst jenes arithmetische Kennzeichen der quadratischen Irrationellen nach Lagrange'schen Gesichtspunkten hergeleitet, nachdem zuvor die elementare Grundlage der Herleitung, die Theorie der Kettenbrüche, zur Vorbereitung auf Jacobi's Arbeit, mittels eines Algorithmus entwickelt worden, von welchem der Jacobi'sche nur eine einfache Verallgemeinerung ist. Dann folgt Liouville's Nachweis von dem Vorhandensein nicht algebraischer Irrationellen und eine kurze Uebersicht der Hauptarbeiten, durch welche Lambert, Legendre und Liouville über die Natur der Zahlen e und π Licht zu verbreiten gesucht haben. Ausführlich stellen wir darauf die Hermite'schen Arbeiten über die Zahl e, wie sie sich finden im Journal für die r. u. a. Mathematik Bd. 76 pag. 303 und 342 und in der Schrift Sur la fonction exponentielle, Paris 1874, in ihrem Zusammenhange dar, und geben dann einen Theil der Lindemannschen Untersuchung über die Ludolph'sche Zahl, soweit es erforderlich ist, um von ihrem Gang und Charakter eine genügende Vorstellung zu bilden; statt sie im Ganzen zu ent-

wickeln, ziehen wir es vor, den Nachweis für die Transcendenz der Zahl π auf dem einfacheren Wege zu erbringen, welchen Herr Weierstrass uns gelehrt hat. Konnte soweit von Untersuchungen berichtet werden, welche zu endgiltigen Ergebnissen geführt haben und als abgeschlossen zu betrachten sind, so giebt eine letzte Vorlesung Kenntniss von den Kettenbruchalgorithmen von Jacobi und von den wenigen, noch unzureichenden Resultaten, zu denen der Versuch, Kennzeichen ähnlich dem für die quadratischen Irrationellen gefundenen auch für die kubischen zu ermitteln, bisher geführt, und bei welchen die Erforschung der Natur der Irrationalzahlen ihren einstweiligen Abschluss gefunden hat.

Weimar, 28. November 1891.

Inhaltsverzeichniss.

Erste Vorlesung.
Definition der Irrationalzahlen.

Zweite Vorlesung.
Ueber algebraische Zahlen.

Dritte Vorlesung.
Die Kettenbrüche.

Vierte Vorlesung.

Die quadratischen Irrationellen.

Fünfte Vorlesung.

Vorhandensein transcendenter Zahlen. — Geschichtliches über die Zahlen e und π.

Sechste Vorlesung.

Hermite's Untersuchung der Zahl e.

Neunte Vorlesung.

Weierstrass'scher Beweis der Transcendenz von π.

Zehnte Vorlesung.

Ueber die kubischen Irrationellen.

Erste Vorlesung.

Definition der Irrationalzahlen.

1. Es ist bekannt, dass die Arithmetik ihren Ausgangspunkt von den positiven ganzen Zahlen nimmt, welche die sogenannte natürliche Zahlenreihe

$$1, 2, 3, 4, 5, 6, \ldots$$

bilden, dass diese jedoch keineswegs ausreichen, um alle arithmetischen Aufgaben zu lösen. Man muss vielmehr zu diesem Zwecke zu den positiven noch die negativen ganzen Zahlen, zu den ganzen Zahlen die gebrochenen hinzunehmen, und erhält so die Gesammtheit der rationalen Zahlen, welche allgemein als Verhältnisse zweier ganzen Zahlen dargestellt werden können. Aber auch mit den rationalen Zahlen kommt man noch nicht aus. Fragen wir z. B. nach der Bedingung, unter welcher die Gleichung

$$x^2 = D, \tag{1}$$

wenn D eine positive Zahl ist, eine rationale Wurzel hat, so kann diese Wurzel entweder eine ganze Zahl $x = n$ sein, und folglich müsste dann D das Quadrat einer ganzen Zahl, $D = n^2$, sein; oder x ist eine gebrochene Zahl, $x = \frac{p}{q}$; dann kann dieser Bruch auf seine kleinste Benennung gebracht, also p, q als zwei ganze Zahlen ohne gemeinsamen Theiler angenommen werden, während q von 1 verschieden ist. Aus der Gleichung (1) ergäbe sich dann

$$p^2 = Dq^2,$$

und folglich müsste jede in q aufgehende Primzahl auch in p enthalten sein, gegen die Voraussetzung. Hiernach kommen

wir zu dem Schlusse: Wenn D nicht das Quadrat einer ganzen Zahl ist, so giebt es keine rationale Zahl, welche die Gleichung (1) befriedigt; im entgegengesetzten Falle ist die rationale Wurzel eine ganzzahlige, nämlich, wenn $D = n^2$ ist, $x = \pm n$.

Wir haben uns zum Beweise dieses bekannten Elementarsatzes auf ein arithmetisches Princip betreffend die Theilbarkeit der ganzen Zahlen gestützt. Man kann aber dasselbe auch ohne dieses Princip nachweisen*), wenn man sich eines Ausdruckes bedient, den wir hier sogleich anführen wollen, da wir auch später von ihm wieder Gebrauch zu machen haben. Dies ist der Ausdruck

$$x^2 - Dy^2,$$

eine sogenannte quadratische Form. Derselbe hat die fundamentale Eigenschaft, dass er, mit einem Ausdrucke gleicher Gestalt multiplicirt, sich wiederherstellt, d. h. wieder in die gleiche Gestalt gebracht werden kann. Es besteht nämlich folgende Identität:

$$(2)\quad (x^2 - Dy^2)\cdot(x'^2 - Dy'^2) = (xx' - Dyy')^2 - D\cdot(xy' - x'y)^2.$$

Angenommen nun, D sei keine Quadratzahl, es existire aber gleichwohl eine rationale Zahl, deren Quadrat gleich D ist, so gäbe es auch zwei positive ganze Zahlen p, q, für welche

$$(3)\quad p^2 - Dq^2 = 0$$

ist; unter allen solchen Systemen sei p, q dasjenige, bei welchem q am kleinsten ist. Nun kann man eine positive ganze Zahl k so wählen, dass

$$k^2 < D < (k+1)^2,$$

folglich

$$(4)\quad kq < p < (k+1)q$$

ist, und demnach die Zahlen

$$p - kq$$

$$p^2 - kpq = Dq^2 - kpq,$$

endlich auch

*) Dedekind, Stetigkeit und irrationale Zahlen, Braunschweig 1872, pag. 20.

$$Dq - kp$$

positiv sind. Setzt man dann in der Formel (2)

$$x = p, \quad y = q, \quad x' = k, \quad y' = 1,$$

so liefert sie folgende Beziehung:

$$(p^2 - Dq^2) \cdot (k^2 - D) = (pk - Dq)^2 - D \cdot (p - qk)^2,$$

oder auch wegen (3):

$$p'^2 - Dq'^2 = 0,$$

wenn unter p', q' die beiden positiven ganzen Zahlen

$$p' = Dq - pk, \quad q' = p - qk$$

verstanden werden, von welchen nach der zweiten der Ungleichheiten (4) $q' < q$ ist, was der Bedeutung von q widerstreitet.

2. Der soeben auf zwiefache Weise bewiesene Satz ist nur der einfachste Specialfall eines weit allgemeineren. Um letzteren einfach aussprechen zu können, betrachten wir irgend eine algebraische Gleichung von beliebigem Grade:

$$ax^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_m = 0,$$

in welcher die Coefficienten ganze Zahlen oder, indem wir den höchsten immer gleich 1 voraussetzen wollen, die Gleichung

$$(5) \qquad x^m + A_1 x^{m-1} + A_2 x^{m-2} + \cdots + A_m = 0,$$

in welcher die Coefficienten rationale Zahlen sind. Die Wurzel jeder solchen Gleichung werden wir mit Kronecker kurz eine algebraische Zahl und, wenn sämmtliche Coefficienten ganzzahlig sind, eine ganze algebraische Zahl nennen. Der Satz, den wir meinen, lautet dann einfach so: **Eine ganze algebraische Zahl ist eine gewöhnliche ganze Zahl, wenn sie rational ist.** Denn, ist $x = \frac{p}{q}$ eine rationale Lösung der Gleichung (5), wobei wieder p, q als zwei ganze Zahlen ohne gemeinsamen Theiler vorausgesetzt werden dürfen, so giebt die Einsetzung dieses Werthes in die Gleichung (5) sofort folgende Beziehung:

$$p^m = -q\,[A_1 p^{m-1} + A_2 p^{m-2} \cdot q + \cdots + A_m q^{m-1}],$$

d. h. p^m gleich einem Vielfachen von q, und demnach wäre p durch jeden in q enthaltenen Primfaktor theilbar, was der An-

nahme über p, q widerstreitet, es sei denn $q = 1$, also $x = p$ eine ganze Zahl.

Hieraus schliessen wir zugleich, dass eine Gleichung von der Art wie (5) mit ganzzahligen Coefficienten, welche keine ganze Wurzel hat, auch keine rationale Wurzel haben kann.

3. Wenn nun eine gegebene Gleichung dieser Art durch keine rationalen Werthe befriedigt wird, so stehen wir vor der Wahl, entweder zu erklären, dass sie keine Lösung zulasse, oder ihre Lösung zu ermöglichen, indem wir neue Zahlen schaffen und einführen, welche dazu geeignet sind, nämlich die irrationalen. Man stösst bekanntlich in der Anwendung überall, schon bei den einfachsten Aufgaben, auf Fälle, welche die Zulassung solcher Zahlen gebieterisch fordern. Man denke nur an ein rechtwinkliges Dreieck, dessen Katheten gleich 2 und 3 Längeneinheiten sind, so wird die Länge x der Hypotenuse durch die Gleichung

$$x^2 = 4 + 9 = 13$$

bestimmt; obwohl also die Hypotenuse selbst eine völlig bestimmte Grösse ist, kann doch ihr Werth so lange nicht angegeben werden, als man sich auf die Betrachtung rationaler Zahlen beschränkt. Aber die Anwendbarkeit eines Begriffes kann im Grunde nicht als eine ausreichende wissenschaftliche Begründung desselben angesehen werden, man muss vielmehr zeigen, dass die Definition des Begriffes von einem ganz bestimmten, vernünftigen Sinne und so der Begriff in sich selbst begründet ist. Und so haben wir also zu fragen: Hat es einen Sinn, eine Zahl x durch die Bedingung z. B. zu definiren, dass $x^2 = 13$ sei, und welches ist dieser Sinn?*)

Eine rationale Zahl x giebt es, wie wir wissen, nicht, die der Gleichung genügte; zunächst aber giebt es unter den ganzen Zahlen zwei, die ihr möglichst nahe genügen, nämlich 3 und 4, jene zu klein, diese zu gross, denn ihre Quadrate sind 9 und 16; desgleichen unter den einstelligen Decimalbrüchen zwei, nämlich 3,6 und 3,7, die möglichst nahe ge-

*) Vgl. zum Folgenden E. Heine, Die Elemente der Funktionenlehre, im J. f. d. r. u. a. Math. Bd. 74.

nügen, jene zu klein, diese zu gross, mit den Quadraten 12,96 und 13,69; ebenso zwei meist genäherte Zahlen unter den zweistelligen Decimalbrüchen, 3,60 und 3,61, etwas zu klein und etwas zu gross, mit den Quadraten 12,9600 und 13,0321 u. s. w. Kurz, es lassen sich zwei unbegrenzte Reihen rationaler Zahlen aufstellen:

$$(6)\quad \begin{cases} 3; & 3{,}6; & 3{,}60; & 3{,}605; & 3{,}6055; & 3{,}60555; & \cdots \\ 4; & 3{,}7; & 3{,}61; & 3{,}606; & 3{,}6056; & 3{,}60556; & \cdots \end{cases}$$

von der Beschaffenheit, dafs zwar die Quadrate der ersteren Zahlen stets zu klein, die Quadrate der letzteren stets zu gross sind, dass jedoch, wenn die Zahlen dieser beiden Reihen nach einander für x eingesetzt werden, die Gleichung $x^2 = 13$ mit stets wachsender Annäherung gelöst, der begangene Fehler stets kleiner wird, und verschwindend klein werden würde, wenn man jede dieser beiden Reihen ins Unendliche fortsetzen würde. Die beiden Reihen haben zudem die Eigenschaft, dass die erstere eine Reihe wachsender, die zweite eine Reihe abnehmender Zahlen ist, und dafs der Unterschied zwischen zwei entsprechenden Gliedern beider Reihen unter jeden Grad von Kleinheit herabsinkt, wenn man die Reihen weit genug fortsetzt. Aus dieser Ursache wollen wir die erstere Reihe die ansteigende, die zweite die absteigende, beide zusammen aber zwei gegen einander convergirende Zahlenreihen nennen.

Aus dem Gesagten geht nun hervor, dass, wenn die Gleichung $x^2 = 13$ durch eine Zahl gelöst wird, diese stets zwischen den sich entsprechenden Gliedern der beiden Zahlenreihen (6) enthalten sein muss, und da die Glieder gegen einander convergiren, d. h. schliesslich sich um weniger von einander unterscheiden, als irgend ein angebbarer Werth, sich von diesen Gliedern selbst um so weniger wird unterscheiden können. Wir dürfen jene Zahl x dann also als den gemeinsamen Grenzwerth beider gegen einander convergirenden Zahlenreihen bezeichnen. Umgekehrt, wenn eine Zahl x existirt, welche stets von diesen beiden Reihen umschlossen wird und daher als ihr gemeinsamer Grenzwerth bezeichnet werden darf, so darf diese auch als eine Lösung der

Gleichung $x^2 = 13$ aufgefasst werden. Wir erkennen hieraus, dass die Annahme einer *Zahl*, welche der Gleichung $x^2 = 13$ genügt, gleichbedeutend ist mit der andern Annahme, dass den beiden gegen einander convergirenden Reihen (6) eine *Zahl* zugehört, die sie zu gemeinsamem Grenzwerthe haben.

4. Wie steht es nun mit der Berechtigung dieser letzteren Auffassung?

Zuerst wollen wir daran erinnern, dass es ganz gang und gäbe ist, rationale Zahlen als solche Grenzwerthe aufzufassen, denn wenn wir z. B. die Zahl $\frac{1}{3}$ durch den unendlichen Decimalbruch 0,33333 ⋯ ersetzen, so heisst das, genau besehen, nichts anderes, als dass wir sie auffassen als den gemeinsamen Grenzwerth der beiden gegen einander convergirenden Zahlenreihen:

$$\begin{array}{llllll} 0; & 0{,}3; & 0{,}33; & 0{,}333; & 0{,}3333; & \cdots \text{ ansteigend,} \\ 1; & 0{,}4; & 0{,}34; & 0{,}334; & 0{,}3334; & \cdots \text{ absteigend} \end{array}$$

zwischen deren sich entsprechenden Gliedern $\frac{1}{3}$ stets enthalten bleibt. In gleicher Weise kann man jede rationale Zahl, und zwar auf mannigfache Weise, als gemeinsamen Grenzwerth zweier gegen einander convergirenden Zahlenreihen auffassen, z. B. die Null als Grenzwerth der beiden Reihen:

$$\begin{array}{lllll} 1, & \frac{1}{2^m}, & \frac{1}{3^m}, & \frac{1}{4^m}, & \cdots \\ -1, & -\frac{1}{2^m}, & -\frac{1}{3^m}, & -\frac{1}{4^m}, & \cdots, \end{array}$$

wenn m positiv ist, und je nachdem man für m diesen oder jenen positiven Werth wählt, würde man verschiedene solche Bestimmungsweisen erhalten.

Zweitens ist uns aber die in Frage gestellte Auffassung überhaupt ganz geläufig. Nehmen wir irgend einen unendlichen Decimalbruch, z. B. denjenigen, bei welchem die ersten Decimalziffern die Zahlen 1 bis 9 sind, auf welche sie dann jedesmal zweifach, dann dreifach wiederholt folgen u. s. w., also:

$$0{,}123456789112233445566778899111222 \cdots$$

Niemand von uns nimmt Anstand, unter demselben eine ganz bestimmte Zahl zu verstehen, obwohl wir nicht wissen, vielmehr ernstlich daran zweifeln dürfen, ob sie durch einen rationalen Werth ausdrückbar sein mag; wir haben uns eben daran gewöhnt, mit solchen unendlichen Brüchen den Sinn einer bestimmten Zahl zu verknüpfen. Im Grunde ist nun aber dieser Sinn des Decimalbruches kein anderer als der, der gemeinsame Grenzwerth für die folgenden zwei gegen einander convergirenden Zahlenreihen zu sein:

$$\begin{array}{ll} 0 & 1 \\ 0{,}1 & 0{,}2 \\ 0{,}12 & 0{,}13 \\ 0{,}123 & 0{,}124 \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \end{array}$$

und sonach verbinden wir also aus Gewohnheit mit diesen beiden Zahlenreihen unbedenklich die Vorstellung einer bestimmten Zahl als ihres gemeinsamen Grenzwerthes. Nun betrachten wir irgend zwei gegen einander convergirende Zahlenreihen

$$(7)\qquad \begin{cases} a_1, & a_2, & a_3, & \cdots & a_i, & \cdots \\ b_1, & b_2, & b_3, & \cdots & b_i, & \cdots, \end{cases}$$

von denen die erstere die ansteigende, die zweite die absteigende sein mag, d. h. zwei Reihen, in denen für jeden Werth des Index i die Bedingungen erfüllt sind:

$$b_i > b_{i+1} > a_{i+1} > a_i$$

und die Differenz $b_i - a_i$ mit wachsendem Index unendlich klein wird. Offenbar wäre es nur eine Verallgemeinerung obiger Auffassung, wenn wir auch von diesen zwei gegen einander convergirenden Werthreihen aussagten, dass sie mit einander eine Zahl als ihren gemeinsamen Grenzwerth bestimmen. Indessen dürfen wir nicht übersehen, dass solche Auffassung zweierlei in sich schliesst: 1) die Annahme, dass beide Reihen thatsächlich eine gemeinsame Grenze haben, d. h. dass etwas existirt, was als gemeinsame Grenze beider vorgestellt werden kann, und 2) dass dies Existirende als eine Zahl betrachtet werden darf. Der Strenge der Arithmetik, welche von allen Theilen der Mathematik als die „reinste“

Wissenschaft gilt, entspräche es wenig, wenn wir ihre fundamentalsten Begriffe auf Axiome, wie die erste, weder erwiesene noch überhaupt nachweisbare Annahme es wäre, begründen würden. Wir stellen uns daher auf einen anderen Standpunkt, den zuerst **Heine** eingenommen hat.*)

Wir stellen in der That die *Definition* auf: Die beiden gegen einander convergirenden Zahlenreihen (7) *bestimmen* mit einander eine Zahl oder es *entspreche* ihnen eine Zahl z. Aber wir ziehen nicht, um sie vorzustellen, den Begriff der Grenze zu Hilfe, sondern fassen sie — zunächst ganz mit **Heine** — rein formell als ein Zahlzeichen, indem wir darunter das Symbol

$$(8) \qquad z = \begin{pmatrix} a_1, & a_2, & a_3, & \cdots & a_i, & \cdots \\ b_1, & b_2, & b_3, & \cdots & b_i, & \cdots \end{pmatrix} = \begin{pmatrix} a_i \\ b_i \end{pmatrix}$$

verstehen, auf. Um diesen allgemeineren Zahlenbegriff in Verbindung zu bringen mit dem gewohnten Begriffe der rationalen Zahlen, setzen wir ferner fest, dass, so oft eine rationale Zahl z vorhanden ist, welche stets zwischen a_i, b_i enthalten bleibt und daher als gemeinsamer Grenzwerth beider Reihen aufgefasst werden darf, *diese Zahl* unter dem Symbole (8) verstanden werden soll. Und endlich nennen wir die durch das Symbol (8) definirte Zahl z allgemein den gemeinsamen Grenzwerth der zwei gegen einander convergirenden Zahlenreihen (7). — Sonach hätten wir die allgemeineren Zahlen nach **Heine**'s Vorgange lediglich als Zahlzeichen definirt. Wollen wir aber diesen formellen Zeichen auch einen realen Sinn untergelegt sehen, so können die rationalen Zahlen uns dazu führen. Eine solche, $\frac{m}{n}$, tritt zunächst auch nur als ein Symbol oder als ein Zahlzeichen auf, durch welches die rationale Zahl als den Zahlen m, n entsprechend bezeichnet wird; es bedeutet aber sodann das Resultat einer Reihe von Operationen, welche an der Einheit vollzogen werden sollen, und enthält demnach in sich den Ausdruck einer ganz bestimmten *Forderung*, ohne Rücksicht übrigens darauf, ob oder wie diese Forderung that-

*) A. a. O.; aus der Einleitung seiner Arbeit ist ersichtlich, dass die Priorität für seine Auffassung im Grunde Herrn G. **Cantor** zukommt.

sächlich erfüllbar ist. Genau ebenso werden wir das unter (8) definirte Zahlzeichen oder die durch die Reihen (7) bestimmte Zahl als den Ausdruck einer bestimmten Forderung auffassen können, nämlich der Forderung, die beiden gegen einander convergirenden Zahlenreihen gleichzeitig unbegrenzt fortzusetzen oder zu durchlaufen.

Der eigentliche Unterschied zwischen der Heine'schen Auffassung der Zahl als das Zahlzeichen (8) und der zuvor erwähnten Auffassung dürfte dann so ausgesprochen werden können: Während wir hier die Zahl als den Ausdruck der genannten Forderung *selbst* definiren, setzt jene Auffassung, nach der sie der gemeinsame Grenzwerth beider Reihen (7) ist, die Zahl als das Resultat der geforderten Operation, als dasjenige fest, zu dem man gelangen würde, wenn man die Forderung erfüllte oder erfüllen, nämlich die Werthreihen ins Unendliche durchlaufen könnte. Diese Festsetzung enthält aber, wie bemerkt, eine Behauptung oder eine Annahme, welche sich nie erweisen lässt, während die Heine'sche von allem Hypothetischen frei ist.

5. Gleichviel nun, ob man den allgemeineren Zahlenbegriff in der angegebenen Weise nur rein formell oder als das Zahlzeichen (8) definirt, oder den von uns angegebenen realen Sinn damit verbinden will, eins bleibt noch zu erörtern, inwiefern man nämlich berechtigt sei, das so Definirte als eine Zahl zu charakterisiren. Zu diesem Zwecke suchen wir klar zu stellen, was bei der Erweiterung des rationalen Zahlenbegriffes noch unter Zahl verstanden werden kann und soll.

Zunächst dürfen wir natürlich nicht verlangen, dass der erweiterte Zahlenbegriff unter die üblichen Definitionen des gewöhnlichen sich einbegreifen lasse; aber umgekehrt muss die rationale Zahl als besonderer Fall in dem erweiterten Zahlenbegriffe enthalten sein. Dieser Forderung nun genügt der Heine'sche allgemeine Zahlenbegriff, denn es ist bemerkt worden, dass jede rationale Zahl als gemeinsamer Grenzwerth zweier gegen einander convergirender Zahlenreihen aufgefasst werden kann. Bedenken wir ferner, dass der alleinige Zweck der Erweiterung des Zahlenbegriffes, schon beim ersten Schritte über die positiven ganzen Zahlen hinaus,

nur der ist, gewisse Rechnungen allgemein ausführbar zu machen, die mit den Zahlen engeren Sinnes allein nicht möglich sind, so darf das wesentliche Merkmal der Zahlen überhaupt darin gesetzt werden, dass sich mit ihnen rechnen lässt, d. h. dass zwei solche Elemente nach bestimmten Regeln wieder zu einem Elemente derselben Art verknüpft werden können. Die für die engere Gattung der rationalen Zahlen fundamentalen Regeln sind die vier Species, die Addition, Subtraction, Multiplication und Division, die bei den rationalen Zahlen in der That (wenigstens nach Ausschluss der Null, welche nur uneigentlich eine Zahl ist) stets wieder eine rationale Zahl liefern.

Wenn wir also jetzt den allgemeineren Zahlenbegriff, wie oben, festsetzen, so müssen wir, um das Definirte wirklich als Zahl bezeichnen zu dürfen, Regeln angeben können, wie zwei solche Zahlen mit einander zu einer dritten verknüpft werden können, die als ihre Summe, Differenz, Produkt oder Quotient angesehen werden darf; damit sie das darf, wird aber nur erforderlich sein, dass, so oft die verknüpften Zahlen rational sind, auch wirklich ihre richtige Summe u. s. w. nach jenen Regeln entsteht; denn die für die allgemeinere Gattung der Zahlen giltigen Regeln müssen selbstverständlich auch für die darin enthaltene besondere Art richtig bleiben.

Wir werden uns bei dieser Betrachtung auf das für unseren Zweck, bei dem es uns nicht auf Vollständigkeit ankommt, Ausreichende beschränken, indem wir voraussetzen, dass die Zahlen beider gegen einander convergirenden Zahlenreihen sämmtlich positiv sind; die Zahl z wird dann auch als positiver Werth bezeichnet werden dürfen.

Sei nun

$$\zeta = \begin{pmatrix} \alpha_1, & \alpha_2, & \alpha_3, & \cdots & \alpha_i, & \cdots \\ \beta_1, & \beta_2, & \beta_3, & \cdots & \beta_i, & \cdots \end{pmatrix}$$

oder kürzer

$$\zeta = \binom{\alpha_i}{\beta_i}$$

eine zweite durch die im Symbol enthaltenen zwei gegen einander convergirenden Zahlenreihen, von denen die obere die an-, die untere die absteigende sei, definirte positive Zahl, so

überzeugt man sich zuerst ohne Mühe, dass dann auch sowohl die beiden Zahlenreihen

$$(9)\qquad \begin{cases} a_1+\alpha_1, & a_2+\alpha_2, & a_3+\alpha_3, & \cdots \\ b_1+\beta_1, & b_2+\beta_2, & b_3+\beta_3, & \cdots \end{cases}$$

als auch die beiden Reihen

$$(10)\qquad \begin{cases} a_1-\beta_1, & a_2-\beta_2, & a_3-\beta_3, & \cdots \\ b_1-\alpha_1, & b_2-\alpha_2, & b_3-\alpha_3, & \cdots \end{cases}$$

als auch endlich die beiden Reihen

$$(11)\qquad \begin{cases} a_1\alpha_1, & a_2\alpha_2, & a_3\alpha_3, & \cdots \\ b_1\beta_1, & b_2\beta_2, & b_3\beta_3, & \cdots \end{cases}$$

je zwei gegen einander convergirende Zahlenreihen sind. Um dies z. B. von der letzten zu zeigen, so folgt aus den charakteristischen Ungleichheiten, nach welchen

$$b_i > b_{i+1} > a_{i+1} > a_i$$
$$\beta_i > \beta_{i+1} > \alpha_{i+1} > \alpha_i$$

ist, um so mehr auch

$$b_i\beta_i > b_{i+1}\beta_{i+1} > a_{i+1}\alpha_{i+1} > a_i\alpha_i;$$

und da $b_i - a_i$ und $\beta_i - \alpha_i$ mit wachsendem Index i unter jeden Grad von Kleinheit herabsinken und

$$b_i\beta_i - a_i\alpha_i = b_i(\beta_i - \alpha_i) + \alpha_i(b_i - a_i)$$

gesetzt werden kann, so gilt dasselbe von $b_i\beta_i - a_i\alpha_i$, weil α_i, b_i endlich, jenes nämlich stets zwischen α_1 und β_1, dieses zwischen a_1, b_1 enthalten bleiben. Diesem zufolge sind die gedachten zwei Zahlenreihen (11) gegen einander convergirend.

Hiernach wollen wir nun die Grenzwerthe der drei Paare gegen einander convergirender Zahlenreihen (9), (10), (11), d. h. die — nach unserer Festsetzung — ihnen entsprechenden Zahlen resp. als Summe, Differenz und Produkt der beiden Zahlen z, ζ definiren, also setzen:

$$(12)\qquad \begin{cases} z+\zeta = \begin{pmatrix} a_i+\alpha_i \\ b_i+\beta_i \end{pmatrix}, \qquad z-\zeta = \begin{pmatrix} a_i-\beta_i \\ b_i-\alpha_i \end{pmatrix} \\ z\cdot\zeta = \begin{pmatrix} a_i\alpha_i \\ b_i\beta_i \end{pmatrix}. \end{cases}$$

6. Es ist leicht einzusehen, dass diese Definitionen der Forderung genügen, auch in dem Falle giltig zu bleiben, dass

die Zahlen z und ζ rationale Zahlen sind. Denn liegt eine rationale Zahl z stets zwischen a_i und b_i, eine andere ζ stets zwischen α_i und β_i, so liegen selbstverständlich $z + \zeta$, $z - \zeta$, $z\zeta$ resp. zwischen den sich entsprechenden Gliedern der gegen einander convergirenden Zahlenreihen (9), (10), (11), und können demnach als mit ihren Grenzwerthen übereinstimmend definirt werden.

Bei der Differenz

$$z - \zeta = \begin{pmatrix} a_i - \beta_i \\ b_i - \alpha_i \end{pmatrix}$$

sind mehrere Fälle möglich. Aus den Ungleichheiten

$$b_i - \alpha_i > b_{i+1} - \alpha_{i+1} > a_{i+1} - \beta_{i+1} > a_i - \beta_i,$$

welche bei ihr bestehen, folgt zuerst, dass, wenn $b_i - \alpha_i$ für einen bestimmten Werth des Index negativ ist, es auch für alle grösseren Werthe desselben so bleibt, und um so mehr dann auch $a_i - \beta_i$; dann sind also die sämmtlichen Zahlen der beiden Zahlenreihen von einer bestimmten Stelle an negativ, und demnach ist dann auch $z - \zeta$ als eine negative Zahl anzusehen und man nennt $z < \zeta$. Wird zweitens $b_i - \alpha_i$ niemals negativ, so ist es vom Anfang an und dauernd positiv; ist dann gleichzeitig $a_i - \beta_i$ wenigstens von einer bestimmten Stelle an positiv, so wird man auch $z - \zeta$ als eine positive Zahl anzusehen haben, und man nennt $z > \zeta$. Wenn dagegen $a_i - \beta_i$ niemals positiv wird, sondern dauernd — und vom Anbeginn — negativ bleibt, so haben wir drittens zwei Zahlenreihen, eine ansteigende, aus negativen Zahlen bestehende, und eine absteigende, aus positiven Zahlen gebildete Reihe, welche demnach die Null immer zwischen sich fassen, und welche ihr auch unendlich nahe kommen, weil der Unterschied zwischen zwei sich entsprechenden Gliedern beider Reihen unter jeden Grad von Kleinheit herabsinkt. In diesem Falle also wird der gemeinsame Grenzwerth der beiden Zahlenreihen die Null sein, man hat $z - \zeta = 0$, oder die beiden Zahlen z, ζ sind einander gleich: $z = \zeta$.

So oft überhaupt die Null als Grenzwerth zweier gegen einander convergirender Zahlenreihen dargestellt wird, muss die ansteigende Reihe aus negativen, die absteigende Reihe

aus positiven Zahlen bestehen, welche unter jeden Grad von Kleinheit herabsinken. Denn, würde z. B. die ansteigende Reihe an einer bestimmten Stelle positiv, so würde sie dauernd es bleiben und sich von der Null entfernen, während die absteigende ihr nicht unendlich nahe kommt, da ihre Glieder über den entsprechenden der absteigenden Reihe bleiben. Die Null wird also nicht von den Reihen eingeschlossen, sie kann nicht ihr gemeinsamer Grenzwerth sein, der vielmehr als eine positive Zahl angesehen werden muss.

Setzen wir in der Differenz $z - \zeta$

$$a_i - \beta_i = -\delta_i, \quad b_i - \alpha_i = \varepsilon_i,$$

so sind, wenn $z = \zeta$, d. h. wenn

$$\binom{\beta_i - \delta_i}{\alpha_i + \varepsilon_i} = \binom{\alpha_i}{\beta_i}$$

ist, dem Obigen zufolge δ_i, ε_i positive Werthe, die mit wachsendem Index i unendlich klein werden, während stets $\delta_i + \varepsilon_i > \beta_i - \alpha_i$ bleibt, und man erhält umgekehrt die Gleichheit

$$\binom{\alpha_i}{\beta_i} = \binom{\beta_i - \delta_i}{\alpha_i + \varepsilon_i} \tag{13}$$

für die Grenzwerthe zweier Paare gegen einander convergirender Werthreihen, von denen das eine Paar α_i, β_i, das andere Paar $\beta_i - \delta_i$, $\alpha_i + \varepsilon_i$ zu entsprechenden Gliedern der an- und absteigenden Reihen hat, wenn δ_i, ε_i positive Werthe bedeuten, welche mit wachsendem i unendlich klein werden.

7. Nach diesen Bemerkungen über die Null, über die Gleichheit zweier Zahlen, und wie sie, falls sie ungleich sind, nach der Grösse geordnet zu denken sind, können wir uns zur Definition des Quotienten wenden, die uns noch fehlt. Wir müssen dabei, gerade wie bei dem Quotienten rationaler Zahlen, voraussetzen, dass der Divisor, er sei ζ, von Null verschieden sei, d. h. also, dass die Zahlen α_i, β_i, welche, wie oben, positiv angenommen werden, nicht mit wachsendem Index unendlich klein werden. Sie bleiben demnach, wie gross i auch werde, jedenfalls immer über einer gewissen endlich angebbaren Zahl γ. Wir definiren nun den Quotienten $\frac{z}{\zeta}$ durch die Gleichheit:

$$(14) \qquad \frac{z}{\zeta} = \begin{pmatrix} a_i \\ \beta_i \\ \frac{b_i}{\alpha_i} \end{pmatrix} = \begin{pmatrix} \frac{a_1}{\beta_1}, & \frac{a_2}{\beta_2}, & \frac{a_3}{\beta_3}, & \dots \\ \frac{b_1}{\alpha_1}, & \frac{b_2}{\alpha_2}, & \frac{b_3}{\alpha_3}, & \dots \end{pmatrix}$$

und haben, um dies als zulässig zu erweisen, offenbar nur zu zeigen, dass die in Parenthesen gesetzten beiden Zahlreihen gegen einander convergirende sind; dass die Definition dann auch für rationale z, ζ giltig bleibt, ersieht man, wie bei den drei anderen Operationen, von selbst. Jene Convergenz aber erkennt man daraus, dass

erstens, weil $b_i > a_i$, $\beta_i > \alpha_i$ also $\frac{1}{\alpha_i} > \frac{1}{\beta_i}$ ist, auch $\frac{b_i}{\alpha_i} > \frac{a_i}{\beta_i}$ ist; dass

zweitens, weil $b_{i+1} < b_i$, $\alpha_{i+1} > \alpha_i$ also $\frac{1}{\alpha_{i+1}} < \frac{1}{\alpha_i}$ ist, auch $\frac{b_{i+1}}{\alpha_{i+1}} < \frac{b_i}{\alpha_i}$, die untere Reihe also eine absteigende ist; dass ebenso

drittens, weil $a_{i+1} > a_i$, $\beta_{i+1} < \beta_i$ also $\frac{1}{\beta_{i+1}} > \frac{1}{\beta_i}$ ist, auch $\frac{a_{i+1}}{\beta_{i+1}} > \frac{a_i}{\beta_i}$, die obere Reihe also eine ansteigende ist; und dass endlich

viertens die Differenz zweier sich entsprechender Glieder

$$\frac{b_i}{\alpha_i} - \frac{a_i}{\beta_i} = \frac{b_i \beta_i - a_i \alpha_i}{\alpha_i \beta_i}$$

mit wachsendem Index i unendlich klein wird, indem der Nenner zuletzt stets grösser bleibt als γ^2, während der Zähler, wie schon früher gezeigt worden, gegen Null convergirt.

8. Nachdem in solcher Weise die vier Species für die Zahlen in erweitertem Sinne so festgestellt worden sind, dass sie auch giltig bleiben, d. h. mit den gewöhnlichen vier Species übereinkommen, so oft die verknüpften Elemente der Rechnung rational sind, dürfen wir nunmehr, dem Gesagten zufolge, das durch zwei gegen einander convergirende Zahlenreihen Definirte und als ihr gemeinsamer Grenzwerth Bezeichnete in der That als eine Zahl auffassen. Aber, weil sie nur in besonderen Fällen rational ist, werden wir sie in den

übrigen Fällen **irrational** nennen müssen; die rationalen und irrationalen Zahlen, welche wir so unter einem gemeinsamen Gesichtspunkte zusammengefasst haben, bilden mit einander das Gebiet aller **reellen** Zahlen.

Eine vollständige Arithmetik der reellen Zahlen müsste nun noch zeigen, dass die fundamentalen Rechnungsregeln, welche für rationale Zahlen gelten, auch in Bestand bleiben für die allgemeinere Zahlengattung, welche sie als besondere Art umfasst; z. B., wenn für ein drittes Paar gegen einander convergirender Zahlenreihen der Grenzwerth $\mathfrak{z}$ heisst, etwa

$$\mathfrak{z} = \begin{pmatrix} \mathfrak{a}_i \\ \mathfrak{b}_i \end{pmatrix},$$

wo also $\mathfrak{a}_i$, $\mathfrak{b}_i$ die sich entsprechenden Glieder der an- und absteigenden Reihe sind, so müsste der bekannte Multiplikationssatz

$$(z \pm \zeta) \cdot \mathfrak{z} = z\mathfrak{z} \pm \zeta\mathfrak{z}$$

nachweisbar sein. Wir wollen diesen Nachweis z. B. für das untere Vorzeichen wirklich erbringen. Da

$$z - \zeta = \begin{pmatrix} a_i - \beta_i \\ b_i - \alpha_i \end{pmatrix}$$

ist, liefert die Definition des Produktes zunächst

$$(z - \zeta) \cdot \mathfrak{z} = \begin{pmatrix} a_i\mathfrak{a}_i - \beta_i\mathfrak{a}_i \\ b_i\mathfrak{b}_i - \alpha_i\mathfrak{b}_i \end{pmatrix}, \tag{15}$$

während

$$z\mathfrak{z} = \begin{pmatrix} a_i\mathfrak{a}_i \\ b_i\mathfrak{b}_i \end{pmatrix}, \qquad \zeta\mathfrak{z} = \begin{pmatrix} \alpha_i\mathfrak{a}_i \\ \beta_i\mathfrak{b}_i \end{pmatrix}$$

also nach der Definition der Differenz

$$z\mathfrak{z} - \zeta\mathfrak{z} = \begin{pmatrix} a_i\mathfrak{a}_i - \beta_i\mathfrak{b}_i \\ b_i\mathfrak{b}_i - \alpha_i\mathfrak{a}_i \end{pmatrix} \tag{16}$$

ist. Aber die allgemeinen Glieder in dem Symbole der Formel (16) lassen sich folgendermassen schreiben:

$$a_i\mathfrak{a}_i - \beta_i\mathfrak{b}_i = (b_i\mathfrak{b}_i - \alpha_i\mathfrak{b}_i) - \mathfrak{b}_i(\beta_i - \alpha_i) - (b_i\mathfrak{b}_i - a_i\mathfrak{a}_i)$$
$$b_i\mathfrak{b}_i - \alpha_i\mathfrak{a}_i = (a_i\mathfrak{a}_i - \beta_i\mathfrak{a}_i) + \mathfrak{a}_i(\beta_i - \alpha_i) + (b_i\mathfrak{b}_i - a_i\mathfrak{a}_i),$$

unterscheiden sich also von denen des Symbols in der Formel (15) um die Werthe

$$-\delta_i = -\mathfrak{b}_i(\beta_i - \alpha_i) - (b_i\mathfrak{b}_i - a_i\mathfrak{a}_i)$$
$$+\varepsilon_i = +\mathfrak{a}_i(\beta_i - \alpha_i) + (b_i\mathfrak{b}_i - a_i\mathfrak{a}_i),$$

welche, die ersteren negativ, die zweiten positiv, mit wachsendem i gegen Null convergiren; das Symbol (16) hat mit andern Worten die Gestalt:

$$\begin{pmatrix}(b_i\mathfrak{b}_i - \alpha_i\mathfrak{b}_i) - \delta_i \\ (a_i\mathfrak{a}_i - \beta_i\mathfrak{a}_i) + \varepsilon_i\end{pmatrix}$$

und bezeichnet daher, nach dem durch die Gleichung (13) ausgesprochenen Satze, denselben Werth, wie das Symbol (15).

Weiter wollen wir nicht gehen; es kam uns nur darauf an, zu zeigen, wie die irrationalen Zahlen genau zu definiren sind, und ihren Charakter als Zahlen wissenschaftlich zu begründen. Dies glauben wir durch das Gesagte ausreichend geleistet zu haben.

Wir wollen nur noch, um auf unsern Ausgangspunkt zurückzukommen, bemerken, dass durch die von uns eingeführten allgemeineren oder irrationalen Zahlen nun wirklich auch der Zweck erreicht wird, die Gleichung $x^2 = 13$ z. B. auflösbar zu machen. Denn bezeichnet man mit x die durch die zwei gegen einander convergirenden Zahlenreihen (6) bestimmte Zahl, so ist der gegebenen Definition des Produktes gemäss x^2 diejenige Zahl, welche den aus den Quadraten der in (6) auftretenden Zahlen gebildeten beiden Reihen entspricht, zwischen deren zusammengehörigen Gliedern aber, wie dort bemerkt, die rationale Zahl 13 stets enthalten bleibt, sodass auch sie als ihr gemeinsamer Grenzwerth aufzufassen und demnach $x^2 = 13$ ist.

Zweite Vorlesung.

Ueber algebraische Zahlen.

1. Wir kehren zum Ausgangspunkte der vorigen Betrachtungen nunmehr zurück, um zu fragen, ob die von uns eingeführten irrationalen Zahlen geeignet und hinreichend

sind, alle Gleichungen, wie die Gleichung (5) voriger Vorlesung zu lösen. Anscheinend nicht; denn z. B. kann man für die Gleichung

$$x^2 + 1 = 0$$

weder einen ganzen noch auch einen rationalen Werth x angeben, der sie auch nur mit irgend einer Annäherung löste, sodass es also offenbar auch nicht gelingen kann, mittels solcher unendlich fortgesetzten Annäherung einen Grenzwerth zu bestimmen, der sie wirklich erfüllte. Die genannte Gleichung hat keine reelle Wurzel. Es ist nun aber das Verdienst von Gauss, zuerst den strengen Beweis erbracht zu haben, dass jede algebraische Gleichung von der Form

$$(1) \qquad x^m + A_1 x^{m-1} + A_2 x^{m-2} + \cdots + A_m = 0$$

wenigstens *dann* eine Lösung hat, wenn man ausser den *reellen* Zahlen auch die sogenannten *complexen* Zahlen zulässt, d. h. die Zahlen von der Form $a + bi$, worin i zur Abkürzung steht für das imaginäre Symbol $\sqrt{-1}$, während a, b reelle Werthe bedeuten. Diese letzteren lassen sich mit beliebiger Annäherung berechnen, besser gesagt, es lassen sich für a sowohl wie für b je zwei gegen einander convergirende Zahlenreihen ermitteln, wie sie im Vorigen betrachtet worden sind, als deren Grenzwerthe a, b anzusehen sind. Die mehr oder weniger zweckmässigen Mittel und Wege hierzu sind zuerst von Lagrange, Fourier und später von Vielen gesucht und angegeben worden und bilden den Gegenstand der sogenannten numerischen Auflösung der Gleichungen. Uns ist es nicht möglich, näher hier darauf einzugehen, es muss uns vielmehr genügen, dass die Gleichung (1) in solcher Weise stets gelöst werden kann auf Grund der zuvor gegebenen Definition der irrationalen Zahlen; und die somit wirklich vorhandenen Lösungen der Gleichungen von jener Form nennen wir, wie schon gesagt, algebraische Zahlen. Sie sind, wie unschwer zu sehen, genau denselben allgemeinen Rechnungsregeln unterworfen wie die reellen Zahlen; jedes Lehrbuch über complexe Grössen bringt darüber das nothwendige; hier wollen wir nur zwei allgemeine Sätze von

algebraischen Zahlen beweisen, welche für die Erkenntniss der Natur solcher Zahlen von Wichtigkeit sind.

2. Seien α, β *zwei* algebraische Zahlen, nämlich α eine Wurzel der Gleichung

$$(1) \qquad x^m + A_1 x^{m-1} + A_2 x^{m-2} + \cdots + A_m = 0,$$

β eine Wurzel der Gleichung

$$(2) \qquad x^n + B_1 x^{n-1} + B_2 x^{n-2} + \cdots + B_n = 0$$

mit rationalen Coefficienten, so wird auch jeder rational aus α und β gebildete Ausdruck eine algebraische Zahl sein. Wir zeigen dies zunächst für die drei Ausdrücke $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$.*)

Bezeichnen wir hierzu das Produkt mn kurz durch p, und mit $\omega_1, \omega_2, \omega_3, \cdots \omega_p$ die p Produkte aus jeder der Potenzen

$$1, \alpha, \alpha^2, \cdots \alpha^{m-1}$$

mit jeder der Potenzen

$$1, \beta, \beta^2, \cdots \beta^{n-1},$$

welche also sämmtlich die Form $\alpha^\mu \beta^\nu$ haben, während μ, ν kleiner sind als m, n resp. Nun sei ω irgend eine der Grössen $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$; dann lässt sich jedes der Produkte

$$\omega\omega_1, \omega\omega_2, \omega\omega_3, \cdots \omega\omega_p$$

auf lineare Weise durch die Grössen $\omega_1, \omega_2, \cdots \omega_p$, nämlich in der Form

$$(3) \qquad k_1\omega_1 + k_2\omega_2 + \cdots + k_p\omega_p$$

mit rationalen Coefficienten k_i ausdrücken. In der That sei ω etwa der Ausdruck $\alpha + \beta$, so findet sich

$$(4) \qquad (\alpha + \beta) \cdot \alpha^\mu \beta^\nu = \alpha^{\mu+1} \cdot \beta^\nu + \alpha^\mu \cdot \beta^{\nu+1}$$

und es sind vier Fälle möglich:

entweder ist $\mu < m - 1$, $\nu < n - 1$; dann ist die rechte Seite der Gleichung (4) die Summe zweier der Grössen $\omega_1, \omega_2, \cdots \omega_p$, die Behauptung also erwiesen;

*) Dieser und der in der folgenden Nummer enthaltene allgemeine Satz und die mitgetheilten Beweise finden sich in Dedekind, sur la théorie des nombres entiers algébriques, Paris 1877 (extrait du Bulletin des sciences mathématiques et astronomiques 1. série t. XI et 2. série t. I) pag. 60.

oder es ist $\mu = m - 1$, $\nu < n - 1$; dann gehört das zweite Glied rechts zu den Grössen ω_i, das erste aber kann mittels der Identität

$$\alpha^m + A_1 \alpha^{m-1} + A_2 \alpha^{m-2} + \cdots + A_m = 0$$

auf die Form

$$- A_1 \cdot \alpha^{m-1} \beta^\nu - A_2 \cdot \alpha^{m-2} \beta^\nu - \cdots - A_m \cdot \alpha^0 \beta^\nu$$

gebracht, d. h. als ein linearer Ausdruck mittels einiger der Grössen ω_i und rationalen Coefficienten dargestellt werden, womit wieder die Behauptung erwiesen ist;

oder es ist $\mu < m - 1$, $\nu = n - 1$, dann führt die Identität

$$\beta^\nu + B_1 \beta^{\nu-1} + B_2 \beta^{\nu-2} + \cdots + B_n = 0$$

zu dem gleichen Ziele;

oder endlich es ist $\mu = m - 1$, $\nu = n - 1$; dann bedarf es nur der Anwendung dieser beiden Identitäten, um die Behauptung als richtig zu beweisen. Da nun die gleichen Betrachtungen auch gelten, wenn ω die Differenz $\alpha - \beta$ oder das Produkt $\alpha\beta$ bedeutet, so lassen sich in allen drei Fällen p Gleichungen aufstellen:

$$\begin{aligned}
\omega\omega_1 &= k_1' \omega_1 + k_2' \omega_2 + \cdots + k_p' \omega_p \\
\omega\omega_2 &= k_1'' \omega_1 + k_2'' \omega_2 + \cdots + k_p'' \omega_p \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\omega\omega_p &= k_1^p \omega_1 + k_2^p \omega_2 + \cdots + k_p^p \omega_p,
\end{aligned}$$

deren sämmtliche Coefficienten k_i^h rational sind, und denen man auch die Gestalt geben kann:

$$(5) \quad \begin{cases}
0 = (k_1' - \omega) \cdot \omega_1 + k_2' \omega_2 + \cdots + k_p' \omega_p \\
0 = k_1'' \omega_1 + (k_2'' - \omega) \cdot \omega_2 + \cdots + k_p'' \omega_p \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
0 = k_1^p \omega_1 + k_2^p \omega_2 + \cdots + (k_p^p - \omega) \cdot \omega_p.
\end{cases}$$

Hier müssen wir nun den Begriff einer Determinante und die einfachsten Sätze über sie voraussetzen. Da die Grössen ω_i nicht sämmtlich Null sind, denn unter ihnen befindet sich auch das Produkt $1 \cdot 1$, so muss, einem solchen Satze zufolge, die Determinante der Gleichungen (5), nämlich der Ausdruck

$$\begin{matrix} k_1' - \omega, & k_2', & \cdots & k_p' \\ k_1'', & k_2'' - \omega, & \cdots & k_p'' \\ \cdot & \cdot & \cdot & \cdot \\ k_1^p, & k_2^p, & \cdots & k_p^p - \omega \end{matrix}$$

gleich Null sein. Das giebt aber, wenn die Determinante entwickelt wird, eine Gleichung von der Form

$$(6) \qquad \omega^p + k_1\omega^{p-1} + k_2\omega^{p-2} + \cdots k_p = 0,$$

deren Coefficienten k_i aus den Grössen k_i^h durch Additionen, Subtraktionen oder Multiplikationen gebildet sind, nothwendig also, eben sowohl wie die k_i^h selbst, rational sind. Mit andern Worten: ω, d. h. jede der drei Grössen $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, ist **eine algebraische Zahl.**

Nebenbei wollen wir bemerken, dass, so oft die A_i und B_i ganze Zahlen, d. h. so oft α und β ganze algebraische Zahlen sind, auch die Coefficienten k_i^h den obigen Erörterungen über die Produkte $\omega\omega_i$ gemäss ganze Zahlen sein werden. In diesem Falle werden demnach auch die Zahlen k_i ganze Zahlen und ω wird eine ganze algebraische Zahl sein. So gewinnt man den Zusatz: Die Summe, die Differenz und das Produkt zweier ganzen algebraischen Zahlen **ist wieder eine ganze algebraische Zahl.**

Gehen wir zu unserm eigentlichen Vorhaben zurück, so können wir weiter bemerken, dass, wenn α eine von 0 verschiedene algebraische Zahl ist, dasselbe auch von $\frac{1}{\alpha}$ gilt. Denn ist α eine Wurzel der Gleichung (1), also

$$\alpha^m + A_1\alpha^{m-1} + A_2\alpha^{m-2} + \cdots + A_{m-1}\alpha + A_m = 0,$$

so ist

$$\left(\frac{1}{\alpha}\right)^m + \frac{A_{m-1}}{A_m}\cdot\left(\frac{1}{\alpha}\right)^{m-1} + \cdots + \frac{A_1}{A_m}\cdot\frac{1}{\alpha} + \frac{1}{A_m} = 0,$$

wo die Division mit A_m gestattet war, weil A_m nicht 0 sein kann, wenn es α nicht ist; d. h. $\frac{1}{\alpha}$ ist Wurzel der Gleichung

$$x^m + \frac{A_{m-1}}{A_m}x^{m-1} + \cdots + \frac{A_1}{A_m}x + \frac{1}{A_m} = 0$$

mit rationalen Coefficienten, w. z. b. w.

Verbindet man diese Bemerkung mit dem zuvor Bewiesenen, so leuchtet ein, dass auch $\frac{\beta}{\alpha}$ eine algebraische Zahl sein muss. Und da jeder aus α und β rational zusammengesetzte Ausdruck entsteht, indem man eine Anzahl Additionen, Subtraktionen, Multiplikationen und Divisionen in gewisser Reihenfolge ausführt, so ist die Behauptung hiermit erwiesen: ein jeder Ausdruck dieser Art ist gleichfalls eine algebraische Zahl.

3. Der zweite allgemeine Satz, den wir beweisen wollen, lautet folgendermassen: Wenn ω Wurzel einer algebraischen Gleichung ist, deren Coefficienten algebraische Zahlen sind, so ist ω selbst eine algebraische Zahl.

Denn besteht die Identität

$$\omega^n + \alpha\omega^{n-1} + \beta\omega^{n-2} + \cdots + \gamma = 0,$$

in welcher $\alpha, \beta, \cdots \gamma$ algebraische Zahlen sind, der Art, dass folgende Identitäten stattfinden:

$$\begin{aligned}
\alpha^a + A_1\alpha^{a-1} + \cdots + A_a &= 0\\
\beta^b + B_1\beta^{b-1} + \cdots + B_b &= 0\\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot &\quad \cdot \quad \cdot\\
\gamma^c + C_1\gamma^{c-1} + \cdots + C_\gamma &= 0,
\end{aligned}$$

in denen die Coefficienten sämmtlich rationale Zahlen sind, und bezeichnet man das Produkt $nab \cdots c$ wieder zur Abkürzung mit p, mit $\omega_1, \omega_2, \cdots \omega_p$ aber die sämmtlichen Produkte von der Form:

$$\omega^{n'} \cdot \alpha^{a'} \cdot \beta^{b'} \cdots \gamma^{c'},$$

in denen die Exponenten resp. kleiner sind als $n, a, b, \cdots c$, so überzeugt man sich ohne Mühe genau wie bei dem Beweise des vorigen Satzes, indem man nur die obigen Identitäten verwendet, dass die p Produkte

$$\omega\omega_1, \quad \omega\omega_2, \quad \cdots \quad \omega\omega_p$$

sämmtlich auf die Form

$$k_1\omega_1 + k_2\omega_2 + \cdots + k_p\omega_p$$

gebracht werden können, während die k_i durch Additionen, Subtraktionen und Multiplikationen aus den $A_i, B_i, \cdots C_i$

entstehen und demnach rational sind. Das giebt wieder p Gleichungen von der Gestalt (5) und als Folgerung eine Gleichung von der Form (6), welche eben zeigt, dass ω eine algebraische Zahl ist.

In dem besonderen Falle, wo $\alpha, \beta, \cdots \gamma$ sämmtlich ganze algebraische Zahlen sind, sind die Coefficienten A_i, $B_i, \cdots C_i$ sämmtlich ganze Zahlen; dem eben Gesagten zufolge werden dann auch sämmtliche Coefficienten in den Gleichungen (5) ganze Zahlen sein, und, wie im vorigen Satze, dasselbe auch gelten von den Coefficienten der Gleichung (6). Hieraus schliesst man den Zusatz: Die Wurzel einer Gleichung, deren Coefficienten *ganze* algebraische Zahlen sind, ist selbst eine *ganze* algebraische Zahl.

Aus dem zweiten der hier bewiesenen allgemeinen Sätze geht hervor, dass eine Zahl durch die Bestimmung, Wurzel einer Gleichung zu sein, deren Coefficienten algebraische Zahlen sind, nicht allgemeiner definirt ist, als durch die Bestimmung, einer Gleichung zu genügen mit rationalen Coefficienten; diese letztere Definition umfasst vielmehr die erstere und kann als die allgemeinste Definition algebraischer Zahlen angesehen werden.

4. Hier lässt sich nun sogleich die Frage aufwerfen, ob die sämmtlichen möglichen Irrationalzahlen, wie sie in voriger Vorlesung eingeführt worden sind und wir sie in dieser Vorlesung nach Gauss noch durch die complexen Zahlen ergänzt haben, unter diese Definition mit einbegriffen sind, oder ob es, mit andern Worten, auch nichtalgebraische Zahlen giebt, welche dann als transcendente Zahlen bezeichnet werden könnten?

Aber eine andere Frage liegt fast noch näher. Bleiben wir bei den algebraischen Zahlen, so können wir ihre Gesammtheit eintheilen nach dem Grade der Gleichung, durch welche sie definirt sind, und können so Irrationellen verschiedener Grade, quadratische, kubische, biquadratische u. s. w. Irrationellen unterscheiden. Das ist aber ein algebraischer Gesichtspunkt und Unterschied, und es entsteht die Frage, welche rein arithmetischen Unterschiede

finden statt zwischen diesen Irrationellen verschiedener Grade? welches sind die arithmetischen Kennzeichen, durch welche die Irrationellen der verschiedenen Grade sich von einander scheiden und einzeln erkennbar sind?

Die erste dieser beiden Fragen ist bereits von der Wissenschaft vollkommen befriedigend beantwortet und von Liouville der Nachweis geliefert worden, dass es in der That auch transcendente Zahlen giebt. In dieser Hinsicht forderten besonders zwei Zahlen die Untersuchung der Mathematiker heraus, die beiden, gewöhnlich mit e und π bezeichneten Zahlen, d. i. die Basis des natürlichen Logarithmensystemes und die Ludolph'sche Zahl, welche den Umfang eines Kreises vom Durchmesser 1 misst. In neuester Zeit erst ist es den Bemühungen von Hermite und von Lindemann gelungen, diese höchst anziehende, wichtige Frage zu lösen: Die Zahlen e und π sind transcendent.

Sehr weit entfernt scheint man dagegen noch von der Lösung der zweiten Frage zu sein. Schon seit geraumer Zeit zwar kennt man ein arithmetisches Kennzeichen für die quadratischen Irrationellen, auch haben andere Untersuchungen die Vermuthung eines ähnlichen Kennzeichens auch für Irrationellen höheren Grades, wenigstens für die kubischen, sehr wahrscheinlich gemacht; aber noch hat man im Grunde ihre verschiedene Natur sehr wenig zu erforschen vermocht. Wenn wir dennoch mit der zweiten Frage beginnen, so geschieht es deshalb, weil jene Untersuchungen sich auf Rechnungen der höheren Analysis gründen und grössere Vorkenntnisse erfordern, während das, was über quadratische Irrationellen herzuleiten ist, nur auf sehr einfachen arithmetischen Betrachtungen beruht; die Besprechung der Irrationellen höherer Ordnung lassen wir bis zum Schlusse der Vorlesungen.

Das Kennzeichen quadratischer Irrationellen ist auch im Grunde so bekannt, dass wir Anstand nehmen müssten, es hier ausführlich herzuleiten, wenn diese Herleitung nicht an sich ein ausreichendes Interesse darböte. Sie steht aber, wie wohl zuerst Lagrange gezeigt hat*), im engsten Zusammen-

*) S. Additions zu Euler, élémens d'Algèbre, traduits de l'allemand, avec des notes et des additions, Pétersb. et Paris 1798, § II: mé-

hange mit der wichtigen Theorie der quadratischen Formen, und so werden wir sie, im Anschluss an die Gedanken von Lagrange, in der Folge darstellen. Zugleich aber bringen wir ihre allgemeine, noch bekanntere Grundlage, die Theorie der Kettenbrüche, zu dem Zwecke zur Darstellung, einen Algorithmus sogleich in seiner einfachsten Art zu lehren, dessen Verallgemeinerung, wie sie zuerst Jacobi betrachtet hat, die richtige Grundlage sein dürfte, um über die Natur der Irrationellen höheren Grades zur Erkenntniss zu kommen.

Dritte Vorlesung.

Die Kettenbrüche.

1. Sind a, a_1 zwei positive Werthe, so kann man stets die Gleichung ansetzen:

$$a = p_0 a_1 + a_2,$$

worin p_0 das grösste in dem Verhältnisse $\frac{a}{a_1}$ enthaltene Ganze, a_2 aber den Rest bezeichnet, welcher bei der Division von a durch a_1 erübrigt. Es ist demnach p_0 eine positive ganze Zahl oder Null, je nachdem $\frac{a}{a_1}$ grösser oder kleiner als die Einheit ist, und a_2 ein positiver Werth kleiner als a_1. Wird nun mit a_1, a_2 in gleicher Weise verfahren und dieselbe Rechnung weiter fortgesetzt, so ergiebt sich eine Reihe von Gleichungen wie folgt:

$$(1)\qquad \begin{cases} a = p_0 a_1 + a_2 \\ a_1 = p_1 a_2 + a_3 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{i-1} = p_{i-1} a_i + a_{i+1} \end{cases}$$

in welcher a_1, a_2, a_3, $\cdots$ abnehmende positive Werthe, p_1, p_2, p_3, $\cdots$ aber sämmtlich positive ganze Zahlen bezeichnen.

thodes pour déterminer les nombres entiers, qui donnent les minima des formules indéterminées à deux inconnues.

Zwei wesentlich verschiedene Fälle können sich darbieten: entweder ist das Verhältniss $\frac{a}{a_1}$ rational oder nicht. Im ersteren Falle können wir es dem Verhältnisse zweier positiven ganzen Zahlen ohne gemeinsamen Theiler, welche α, α_1 heissen mögen, gleichsetzen:

$$\frac{a}{a_1} = \frac{\alpha}{\alpha_1}. \tag{2}$$

Für die ganzen Zahlen α, α_1 muss die angedeutete Rechnung eine Reihe von Gleichungen ergeben von der Form:

$$\left\{\begin{array}{ll} \alpha & = p_0\alpha_1 + \alpha_2 \\ \alpha_1 & = p_1\alpha_2 + \alpha_3 \\ \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \alpha_{i-1} & = p_{i-1}\alpha_i \quad , \end{array}\right. \tag{3}$$

worin jetzt die Reste α_k eine abnehmende Reihe ganzer Zahlen bilden, welche nothwendig abbricht, sodass ein Rest — wir haben angenommen α_{i+1} — der Null gleich wird; der vorhergehende Rest α_i muss dann, da er offenbar gemeinsamer Theiler von α, α_1 ist, nach der Voraussetzung gleich 1 sein. Nun folgt aus (2) die Gleichheit der beiden Verhältnisse $\frac{a}{\alpha}$, $\frac{a_1}{\alpha_1}$; wird ihr gemeinsamer Werth q genannt und $q \cdot \alpha_k = a_k$ gesetzt, so ergiebt sich aus (3) folgende neue Reihe von Gleichungen:

$$\left\{\begin{array}{ll} a & = p_0 a_1 + a_2 \\ a_1 & = p_1 a_2 + a_3 \\ \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{i-2} & = p_{i-2}a_{i-1} + a_i \\ a_{i-1} & = p_{i-1}a_i \quad , \end{array}\right. \tag{1'}$$

welche für den vorliegenden Fall den Algorithmus (1) für die Zahlen a, a_1 darstellen, da $p_0, p_1, p_2, \cdots$ die grössten Ganzen bedeuten, die in den Verhältnissen $\frac{\alpha}{\alpha_1} = \frac{a}{a_1}$, $\frac{\alpha_1}{\alpha_2} = \frac{a_1}{a_2}$, $\cdots$ enthalten sind. Ist also $\frac{a}{a_1}$ ein rationales Verhältniss, so besteht der Algorithmus (1) nur aus einer endlichen Anzahl von Gleichungen von der Form (1′).

Ist dagegen $\frac{a}{a_1}$ ein irrationales Verhältniss, so ist die Anzahl der Gleichungen (1) **unbeschränkt**; denn offenbar kann die Rechnung solange immer noch um eine Stelle weitergeführt werden, als keine der Zahlen $a_2, a_3, \cdots$ gleich Null wird, und dieser Fall kann jetzt nicht eintreten; denn würde z. B. $a_{i+1} = 0$, so würde aus der Gleichung $a_{i-1} = p_{i-1}a_i + a_{i+1}$ das Verhältniss $\frac{a_{i-1}}{a_i}$ und damit auch alle vorhergehenden Verhältnisse $\frac{a_{i-2}}{a_{i-1}}, \frac{a_{i-3}}{a_{i-2}}, \cdots$ bis zum letzten $\frac{a}{a_1}$, dies gegen die Voraussetzung, rational werden. Man kann hiernach in diesem Falle passend schreiben:

$$(1'') \qquad \begin{cases} a = p_0a_1 + a_2 \\ a_1 = p_1a_2 + a_3 \\ a_2 = p_2a_3 + a_4 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{cases}$$

Für einen rationalen Werth $\frac{a}{a_1}$ findet man aus den Gleichungen (1') durch successives Fortschaffen der Verhältnisse $\frac{a_1}{a_2}, \frac{a_2}{a_3}, \cdots$ seine Entwicklung in einen **Kettenbruch**:

$$\frac{a}{a_1} = p_0 + \cfrac{1}{p_1 + \cfrac{1}{p_2 + \cdots + \cfrac{1}{p_{i-1}}}},$$

wofür wir der grösseren Bequemlichkeit wegen das Symbol

$$(4) \qquad \frac{a}{a_1} = (p_0; p_1, p_2, \cdots p_{i-1})$$

setzen wollen. Dabei soll p_0, welches eine positive ganze Zahl oder die Null sein konnte, während alle andern p wesentlich positive ganze Zahlen waren, das **Anfangsglied**, die letztern die **Theilnenner** genannt werden, sodass der Satz gilt: **Jede (positive) rationale Zahl kann in einen endlichen Kettenbruch entwickelt werden, dessen sämmtliche Theilnenner positive ganze Zahlen, dessen Theilzähler der positiven Einheit gleich sind.**

Auch jede (positive) Irrationalzahl $\frac{a}{a_1}$ kann aus den Gleichungen (1'') in einen ähnlichen Kettenbruch entwickelt

werden, dessen Gliederzahl beliebig gross gemacht werden kann. Denn, bricht man die Reihe jener Gleichungen bei der Gleichung

$$a_{i-1} = p_{i-1} a_i + a_{i+1}$$

ab, so findet sich die Kettenbruchentwicklung:

$$\frac{a}{a_1} = \left(p_0;\ p_1,\ p_2,\ \cdots\ p_{i-1},\ \frac{a_i}{a_{i+1}}\right),$$

welche sich von der vorigen nur darin unterscheidet, dass zu den ganzzahligen Theilnennern ein Schlussnenner hinzutritt, der eine Irrationalzahl ist, worauf eben die Möglichkeit beruht, die Entwicklung, wenn man will, noch weiter fortzusetzen.

Die Brüche

$$(p_0) = \frac{p_0}{1}, \quad (p_0;\ p_1) = p_0 + \frac{1}{p_1},$$

$$(p_0;\ p_1,\ p_2) = p_0 + \cfrac{1}{p_1 + \cfrac{1}{p_2}}$$

u. s. w., welche aus dem Kettenbruche dadurch entstehen, dass man ihn bei seinen einzelnen Gliedern abbricht, werden seine aufeinanderfolgenden (der erste, zweite, dritte u. s. w.) **Näherungsbrüche** genannt.

2. Nehmen wir $\frac{a}{a_1}$ als gegeben an, so ist damit die **Scala** der Zahlen $p_0,\ p_1,\ p_2,\ \cdots$ ebenfalls bestimmt. Vermittelst dieser Scala wollen wir nun neben den Gleichungen (1') resp. (1'') folgendes neue, nach demselben Gesetze gebildete System von Gleichungen einführen:

$$\text{(X)} \quad \begin{cases} x = p_0 x_1 + x_2 \\ x_1 = p_1 x_2 + x_3 \\ x_2 = p_2 x_3 + x_4 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_{k-1} = p_{k-1} x_k + x_{k+1}\,. \end{cases}$$

Die Anzahl k dieser Gleichungen darf im Falle eines irrationalen Verhältnisses $\frac{a}{a_1}$ beliebig gross angenommen werden, kann dagegen im Falle eines rationalen Verhältnisses nicht grösser sein als die Anzahl der in der Scala vorhandenen

Zahlen p. Wir können nun entweder für x, x_1 beliebige Werthe wählen, und dann werden die nachfolgenden Grössen $x_2, x_3, \cdots x_{k+1}$ durch die Gleichungen (X) mitbestimmt sein; oder aber wir können auch x_k, x_{k+1} beliebig wählen, und dann werden alle vorhergehenden Grössen $x, x_1, x_2, \cdots x_{k-1}$ durch die Gleichungen (X) mitbestimmt sein. Um z. B. x durch x_k, x_{k+1} auszudrücken, hat man nur nöthig, in die erste der Gleichungen (X) den Werth für x_1 einzusetzen, wodurch

$$x = (p_0 p_1 + 1) x_2 + p_0 x_3$$

hervorgeht, darauf in diese Gleichung für x_2 seinen Werth zu setzen, was

$$x = \left((p_0 p_1 + 1) p_2 + p_0\right) \cdot x_3 + (p_0 p_1 + 1) \cdot x_4$$

ergiebt u. s. f., bis alle Zwischengrössen bis x_{k-1} einschliesslich fortgeschafft sind. Da bei diesen aufeinanderfolgenden Substitutionen nirgends andere Rechnungen auszuführen sind als Additionen und Multiplikationen mit den positiven ganzen Zahlen $p_0, p_1, p_2, \cdots$, so müssen in der auf solche Weise entstehenden Gleichung

$$(5) \qquad x = c_k x_k + d_k x_{k+1}$$

die Coefficienten c_k, d_k nothwendig positive ganze Zahlen sein; und Gleiches gilt von den Coefficienten c_k', d_k' in der Gleichung

$$(5) \qquad x_1 = c_k' x_k + d_k' x_{k+1},$$

welche auf demselben Wege erhalten wird, wenn man von der zweiten Formel des Systemes (X) ausgeht. Hierbei ist zwar der Natur der Sache nach $k > 2$ vorausgesetzt, jedoch kann in den Formeln (5) auch $k = 1$ angenommen werden, wenn man dann nur den Coefficienten die Werthe

$$(6) \qquad c_1 = p_0, \quad d_1 = 1, \quad c_1' = 1, \quad d_1' = 0$$

beigelegt denkt.

Den Formeln (5) analog bestehen nun auch die folgenden beiden, vorausgesetzt, dass $k > 1$ ist:

$$(7) \qquad \begin{cases} x = c_{k-1} x_{k-1} + d_{k-1} x_k \\ x_1 = c_{k-1}' x_{k-1} + d_{k-1}' x_k. \end{cases}$$

Aber, indem man in den Gleichungen (5) für x_{k+1} seinen, aus der letzten der Gleichungen (X) folgenden Werth einsetzt, findet man andererseits die Formeln:

$$x = d_k x_{k-1} + (c_k - p_{k-1} d_k) x_k$$
$$x_1 = d'_k x_{k-1} + (c'_k - p_{k-1} d'_k) x_k\,,$$

welche mit den vorhergehenden übereinstimmend sein müssen und daher zu den Beziehungen

$$d_k = c_{k-1}\,, \qquad c_k = p_{k-1} d_k + d_{k-1}\,,$$
$$d'_k = c'_{k-1}\,, \qquad c'_k = p_{k-1} d'_k + d'_{k-1}$$

hinführen. Hierin ist, der Herleitung gemäss, $k > 1$ vorauszusetzen; wird aber sogar $k > 2$ angenommen, so gestattet die Verbindung der vorstehenden Gleichungen die folgenden abzuleiten:

$$(8) \qquad c_k = p_{k-1} c_{k-1} + c_{k-2}\,, \qquad c'_k = p_{k-1} c'_{k-1} + c'_{k-2}\,,$$

welche zur allmählichen Bildung der Coefficienten c_k, c'_k aus je zwei vorhergehenden dienen. Nun findet man aber aus dem Systeme (X) ohne Mühe, dass $c_2 = p_1 p_0 + 1$, $c'_2 = p_1$ ist. Giebt man daher den Zeichen c_0, c'_0 die Werthe

$$(9) \qquad c_0 = 1\,, \quad c'_0 = 0\,,$$

so leuchtet ein, dass das Bildungsgesetz für die Grössen c_k, c'_k, welches die Formeln (8) aussprechen, auch noch für den Index $k = 2$ bestehen bleibt.

Für die Unbestimmten x_k, x_{k+1} wollen wir nun die Werthe 1, 0 resp. wählen; dann werden offenbar nach den Gleichungen (X) x_{k-1}, x_{k-2}, $\cdots$ x_2, x_1, x positive ganze Zahlen werden und eine zunehmende Reihe bilden, woraus von selbst folgt, dass p_0, p_1, p_2, $\cdots$ die grössten Ganzen, x_2, x_3, $\cdots$ die Reste sein werden, welche bei der Division von x durch x_1, von x_1 durch x_2 u. s. f. sich finden, und da unter den letztern der Rest $x_k = 1$ auftritt, müssen die der gemachten Annahme entsprechenden Werthe von x, x_1 relative Primzahlen, d. i. Zahlen ohne gemeinsamen Theiler sein. Diese Werthe sind aber nach den Gleichungen (5) $x = c_k$, $x_1 = c'_k$ resp., daher wir schliessen:

Die Zahlen c_k, c'_k sind relative Primzahlen und

$$\frac{c_k}{c'_k} = (p_0;\, p_1,\, p_2,\, \cdots\, p_{k-1}),$$

d. h. c_k und c'_k sind Zähler und Nenner des k^{ten} Näherungsbruches für den $\frac{a}{a_1}$ darstellenden Kettenbruch, wenn dieser Näherungsbruch auf seinen einfachsten Ausdruck als Quotient zweier Zahlen ohne gemeinsamen Theiler gebracht gedacht wird. Die Gleichungen (8) enthalten somit das Bildungsgesetz für die Zähler und Nenner der aufeinanderfolgenden Näherungsbrüche und lassen sich in Worten ausdrücken wie folgt:

Denkt man sich die Näherungsbrüche auf ihre einfachsten Ausdrücke gebracht, so erhält man den Zähler des k^{ten} Näherungsbruches, wenn man den $(k-1)^{\text{ten}}$ Theilnenner mit dem Zähler des vorhergehenden Näherungsbruches multiplicirt und dazu den Zähler des zweitvorhergehenden Näherungsbruches addirt. Den Nenner findet man nach demselben Gesetze aus den Nennern der beiden voraufgehenden Näherungsbrüche.

Unter diese Regel lässt sich auch der zweite Näherungsbruch schon begreifen, wenn, dem Obigen zufolge, ein fictiver Näherungsbruch der 0ten Ordnung, $\frac{c_0}{c'_0} = \frac{1}{0}$, hinzugedacht wird, dem natürlich kein Werth, sondern nur eine rein schematische Bedeutung zukommt.

3. Bis hierher haben wir die Gleichungen (X) durchweg benutzt, um x und x_1 durch die beiden letzten Unbestimmten x_k, x_{k+1} auszudrücken. Es ist aber schon bemerkt worden, dass auch das Umgekehrte möglich ist. Schafft man zunächst x_k aus der vorletzten Gleichung durch Einsetzen seines Werthes fort, so kommt

$$x_{k+1} = -p_{k-1}x_{k-2} + (p_{k-1}p_{k-2} + 1)x_{k-1}.$$

Wird nun für x_{k-1} sein Werth gesetzt, so findet sich

$$x_{k+1} = (p_{k-2}p_{k-1} + 1)\cdot x_{k-3} - (p_{k-3}(p_{k-2}p_{k-1} + 1) + p_{k-1})\cdot x_{k-2}$$

u. s. w. Schliesslich ergiebt sich eine Formel

$$x_{k+1} = m_{k+1}\cdot x + m'_{k+1}\cdot x_1, \tag{10}$$

in welcher die Coefficienten m_{k+1}, m'_{k+1} positive oder negative ganze Zahlen sein müssen, weil bei jenen aufeinander-

folgenden Substitutionen niemals Divisionen auszuführen sind; und auf demselben Wege findet sich

$$x_k = m_k \cdot x + m'_k \cdot x_1 . \tag{10}$$

Nun hat man aber umgekehrt nach (7):

$$x = c_k \cdot x_k + c_{k-1} \cdot x_{k+1}$$
$$x_1 = c'_k \cdot x_k + c'_{k-1} \cdot x_{k+1} ,$$

zwei Gleichungen, aus deren Auflösung sich

$$x_k = \frac{c'_{k-1} \cdot x - c_{k-1} \cdot x_1}{c_k c'_{k-1} - c'_k c_{k-1}}$$
$$x_{k+1} = \frac{- c'_k \cdot x + c_k \cdot x_1}{c_k c'_{k-1} - c'_k c_{k-1}}$$

ergiebt. Die Vergleichung der letzten Gleichungen, welche dasselbe sein müssen wie die Gleichungen (10), mit diesen letztgenannten, beweist, da m_{k+1}, m'_{k+1} ganze Zahlen waren, dass c_k, c'_k theilbar sind durch $c_k c'_{k-1} - c'_k c_{k-1}$; sie sind aber relative Primzahlen, also muss

$$c_k c'_{k-1} - c'_k c_{k-1} = \pm 1$$

sein. Um über das Vorzeichen zu entscheiden, ersetzen wir c_k und c'_k durch ihre Werthe (8), wodurch die Recursionsformel

$$c_k c'_{k-1} - c'_k c_{k-1} = - (c_{k-1} c'_{k-2} - c'_{k-1} c_{k-2})$$

gewonnen wird. Wenn darin k in $k-1$, $k-2$, $\cdots$ verwandelt wird, in welcher Richtung man soweit fortgehen kann, als die Gleichungen (8) und (10), auf welche wir uns gestützt haben, Geltung behalten, d. h. bis $k = 2$, so entsteht eine Reihe von $k-1$ Gleichungen, deren Multiplikation

$$c_k c'_{k-1} - c'_k c_{k-1} = (-1)^{k-1} \cdot (c_1 c'_0 - c_0 c'_1)$$

oder einfacher

$$c_k c'_{k-1} - c'_k c_{k-1} = (-1)^k \tag{11}$$

ergiebt.

Aus dieser wichtigen Gleichung findet man ferner durch Division mit $c'_{k-1} \cdot c'_k$

$$\frac{c_k}{c'_k} - \frac{c_{k-1}}{c'_{k-1}} = \frac{(-1)^k}{c'_{k-1} \cdot c'_k} , \tag{12}$$

d. h. den Satz: Der Unterschied zwischen zwei aufeinanderfolgenden Näherungsbrüchen ist ein Bruch, dessen Zähler der positiven oder negativen Einheit gleich, dessen Nenner das Produkt aus den Nennern beider Näherungsbrüche ist. Auch schliesst man aus der Formel (12), dass dieser Unterschied mit wachsendem Index k fort und fort abnimmt, wenn man bedenkt, dass die Zähler und Nenner der Näherungsbrüche ihrem Bildungsgesetze gemäss mit dem Index k zugleich wachsen.

Die soeben abgeleiteten Ergebnisse lassen den Grund für die Wahl der Benennung „Näherungsbrüche" erkennen. Verbinden wir nämlich die Gleichungen

$$x = c_k x_k + c_{k-1} x_{k+1}, \quad x_1 = c'_k x_k + c'_{k-1} x_{k+1}$$

mit den andern:

$$a = c_k a_k + c_{k-1} a_{k+1}, \quad a_1 = c'_k a_k + c'_{k-1} a_{k+1},$$

welche auf die analoge Weise aus den Gleichungen (1) gewonnen werden, so finden wir mit Hilfe der Gleichung (11)

$$(13) \qquad a x_1 - a_1 x = (-1)^k \cdot (a_k x_{k+1} - a_{k+1} x_k),$$

eine Beziehung, von welcher man verschiedenen Gebrauch machen kann. Gegenwärtig wollen wir darin $x_k = 1$, $x_{k+1} = 0$ wählen. Dieser Wahl der letzten beiden Unbestimmten entsprechen aber die Werthe $x = c_k$, $x_1 = c'_k$, und folglich liefert so die vorstehende Gleichung die folgende:

$$a c'_k - a_1 c_k = (-1)^{k-1} \cdot a_{k+1}$$

oder auch diese:

$$(14) \qquad \frac{a}{a_1} - \frac{c_k}{c'_k} = \frac{(-1)^{k-1} \cdot a_{k+1}}{a_1 c'_k}.$$

Nun nehmen aber die Grössen $a, a_1, a_2, \cdots$ fort und fort ab, während die Zahlen c'_k, wie zuvor bemerkt, mit wachsendem Index gleichfalls wachsen. Daher ergiebt sich der Satz:

Die aufeinanderfolgenden Näherungsbrüche nähern sich dem Werthe des Kettenbruches mehr und mehr, während dieser Werth stets *zwischen* zwei aufeinanderfolgenden Näherungsbrüchen enthalten bleibt. Diejenigen nämlich, deren Index eine gerade Zahl ist, sind

stets grösser, die andern mit ungeradem Index stets kleiner als der Werth des ganzen Kettenbruchs.

Auch lässt sich das Gesetz der Annäherung aus der Formel (14) sogleich entnehmen. Da nämlich alle in dem Ausdrucke $a_1 = c'_k a_k + c'_{k-1} a_{k+1}$ vorkommenden Zeichen positive Werthe bedeuten, und $a_{k+1} < a_k$ ist, so besteht offenbar die Ungleichheit $a_1 > c'_k a_k > c'_k a_{k+1}$ oder $\frac{a_{k+1}}{a_1} < \frac{1}{c'_k}$. Hiernach liefert die Gleichung (14) das Ergebniss: dass der Unterschied zwischen dem Kettenbruche und seinem k^{ten} Näherungsbruche kleiner ist als $\frac{1}{c'^2_k}$; ein Satz, der auch aus dem Umstande geschlossen werden kann, dass der Werth des Kettenbruches immer zwischen zwei aufeinanderfolgenden Näherungsbrüchen enthalten ist. Denn, da er demnach auch zwischen dem k^{ten} und $(k+1)^{\text{ten}}$ enthalten ist, deren Unterschied numerisch gleich $\frac{1}{c'_k c'_{k+1}}$, also kleiner als $\frac{1}{c'^2_k}$ ist, kann er sich von jeder der beiden Grenzen auch nur um eine Grösse $< \frac{1}{c'^2_k}$ unterscheiden.

Man kann übrigens dies Ergebniss auch in der folgenden Form aussprechen: Der Unterschied $c_k - \frac{a}{a_1} \cdot c'_k$ ist numerisch kleiner als $\frac{1}{c'_k}$, und unter dieser Form kann es zu einer sehr wichtigen Anwendung benutzt werden, welche wir hier kurz erwähnen wollen. In der Zahlentheorie spielt die sogenannte Pell'sche Gleichung

$$x^2 - Dy^2 = 1$$

eine grosse Rolle. Es wird daselbst gezeigt, dass, wenn D eine positive, von einem Quadrate verschiedene ganze Zahl ist, die Pell'sche Gleichung unendlich viele ganzzahlige Lösungen $x = t$, $y = u$ hat, welche sämmtlich aus einer Fundamentalauflösung, derjenigen Auflösung nämlich, für welche x, y die kleinsten positiven Werthe T, U besitzen, vermittelst der Formel

$$t + u\sqrt{D} = \pm (T + U\sqrt{D})^n$$

gefunden werden, wenn man dem n allmählich alle ganzzahligen Werthe beilegt, der Reihe nach sowohl das obere als das untere Vorzeichen nimmt und jedesmal die rationalen Theile sowie die irrationalen Theile rechts und links gleichsetzt. Die Grundlage dieses Nachweises ist aber die Thatsache, dass es unendlich viele ganze Zahlen x, y giebt, für welche

$$x - y\sqrt{D} \text{ numerisch } < \frac{1}{y}$$

ist. Und diese Thatsache wird durch den obigen Satz sogleich als richtig erkannt, wenn man $a = \sqrt{D}$, $a_1 = 1$ wählt. Denn die Zähler und Nenner der Näherungsbrüche des Kettenbruches für $\sqrt{D}$ bilden dann unendlich viel Systeme $x = c_k$, $y = c_k'$ von der angegebenen Beschaffenheit.

4. Im vorigen haben wir immer nur endliche Kettenbrüche betrachtet; denn auch in dem Falle eines irrationalen Verhältnisses $\frac{a}{a_1}$ dachten wir uns doch den Algorithmus (1″) stets nur bis zu einer zwar beliebigen aber bestimmten Stelle hin fortgesetzt. Nun werde jedoch eine ganz beliebige unendlich fortlaufende Reihe positiver ganzer Zahlen $p_0, p_1, p_2, \cdots$, deren erste auch Null sein kann, als gegeben angesehen und der unendliche Kettenbruch

$$\text{(K)} \qquad (p_0;\ p_1,\ p_2,\ p_3,\ \cdots)$$

betrachtet. Es fragt sich vor allem, stellt ein solcher einen bestimmten Werth vor oder nicht? Bricht man ihn an einer bestimmten Stelle p_n ab, so erhält man den endlichen Werth $\frac{c_n}{c_n'}$; die Frage ist demnach, ob $\frac{c_n}{c_n'}$ mit unendlich wachsendem Index n gegen einen Grenzwerth convergirt. Betrachten wir hierzu die beiden unbegrenzten Zahlenreihen

$$\frac{c_1}{c_1'},\quad \frac{c_3}{c_3'},\quad \ldots\quad \frac{c_{2n+1}}{c_{2n+1}'},\quad \ldots$$

$$\frac{c_2}{c_2'},\quad \frac{c_4}{c_4'},\quad \ldots\quad \frac{c_{2n+2}}{c_{2n+2}'},\quad \ldots$$

Nach Gleichung (12) findet sich

$$\frac{c_{2n}}{c'_{2n}} - \frac{c_{2n-1}}{c'_{2n-1}} = \frac{1}{c'_{2n}c'_{2n-1}}$$

$$\frac{c_{2n+1}}{c'_{2n+1}} - \frac{c_{2n}}{c'_{2n}} = \frac{-1}{c'_{2n+1}c'_{2n}}$$

$$\frac{c_{2n+2}}{c'_{2n+2}} - \frac{c_{2n+1}}{c'_{2n+1}} = \frac{1}{c'_{2n+2}c'_{2n+1}}$$

und hieraus weiter

$$\frac{c_{2n+1}}{c'_{2n+1}} - \frac{c_{2n-1}}{c'_{2n-1}} = \frac{1}{c'_{2n}} \cdot \left(\frac{1}{c'_{2n-1}} - \frac{1}{c'_{2n+1}}\right) > 0$$

$$\frac{c_{2n+2}}{c'_{2n+2}} - \frac{c_{2n}}{c'_{2n}} = \frac{1}{c'_{2n+1}} \left(\frac{1}{c'_{2n+2}} - \frac{1}{c'_{2n}}\right) < 0.$$

Diese Beziehungen kennzeichnen aber die beiden Zahlenreihen als zwei positive gegen einander convergirende Zahlenreihen, die erste als wachsende, die zweite als abnehmende, und demnach bestimmen sie eine gewisse endliche positive Zahl ω als ihren gemeinsamen Grenzwerth. Hieraus schliessen wir, dass der unendliche Kettenbruch (K) einen endlichen bestimmten Werth ω hat, und er ist offenbar grösser als 1, sobald das Anfangsglied p_0 von Null verschieden ist. Dasselbe wird aber in gleicher Weise gelten auch von den aus (K) dadurch entstehenden Kettenbrüchen, dass man ein oder mehrere aufeinanderfolgende Glieder am Anfange unterdrückt.

Aus der Gleichung

$$\omega = p_0 + \frac{1}{(p_1;\ p_2,\ p_3,\ \cdots)}$$

folgt sodann p_0 als das grösste in $\frac{\omega}{1}$ enthaltene Ganze. Setzt man demnach

$$\omega = 1 \cdot p_0 + a_2,$$

so ist

$$\frac{1}{a_2} = p_1 + \frac{1}{(p_2;\ p_3,\ p_4,\ \cdots)}$$

und folglich p_1 das grösste in $\frac{1}{a_2}$ enthaltene Ganze; also, wenn

$$1 = p_1 a_2 + a_3$$

gesetzt wird, so findet sich

$$\frac{a_2}{a_3} = p_2 + \frac{1}{(p_3;\, p_4,\, p_5,\, \cdots)}$$

und demnach p_2 als das grösste in $\frac{a_2}{a_3}$ enthaltene Ganze u. s. w. Es ergiebt sich mit anderen Worten als der dem Verhältnisse $\frac{\omega}{1}$ entsprechende Algorithmus (1) die unendliche Reihe von Gleichungen:

$$(\Omega)\qquad \begin{aligned} \omega &= 1 \cdot p_0 + a_2 \\ 1 &= a_2 p_1 + a_3 \\ a_2 &= a_3 p_2 + a_4 \\ &\cdots\cdots \end{aligned}$$

5. Nach dieser allgemeinen Erörterung wollen wir nun eine Gattung unendlicher Kettenbrüche genauer betrachten, welche in arithmetischer Beziehung von besonderem Interesse sind, die periodischen Kettenbrüche. Nehmen wir an, in der unendlichen Reihe von Gleichungen (Ω) kehre von einem bestimmten Theilnenner p_n an stets dieselbe Reihe von Theilnennern $p_n,\ p_{n+1},\ p_{n+2},\ \cdots\ p_{n+m-1}$ wieder, so wird der Kettenbruch ein periodischer:

$$(p_0;\, p_1,\, \cdots\, p_{n-1},\, p_n,\, p_{n+1},\, \cdots\, p_{n+m-1},\, p_n,\, p_{n+1},\, \cdots\, p_{n+m-1},\, \cdots),$$

und jene Reihe von Theilnennern seine Periode genannt. Rein periodisch heisst der Kettenbruch, wenn die Periodicität sogleich mit dem Anfangsgliede p_0 beginnt. Nun findet man aus den n ersten Gleichungen (Ω)

$$(15)\qquad \begin{cases} \omega = c_n a_n + c_{n-1} a_{n+1} \\ 1 = c'_n a_n + c'_{n-1} a_{n+1}, \end{cases}$$

und aus den folgenden m Gleichungen, nämlich

$$\begin{aligned} a_n &= p_n a_{n+1} + a_{n+2} \\ a_{n+1} &= p_{n+1} a_{n+2} + a_{n+3} \\ &\cdots\cdots\cdots\cdots \\ a_{n+m-1} &= p_{n+m-1} a_{n+m} + a_{n+m+1}, \end{aligned}$$

nach demselben Raisonnement die Formeln

$$\begin{aligned} a_n &= C_m a_{n+m} + C_{m-1} a_{n+m+1} \\ a_{n+1} &= C'_m a_{n+m} + C'_{m-1} a_{n+m+1}, \end{aligned}$$

in welchen C_m, C'_m, $\cdots$ ebenso aus p_n, p_{n+1}, $\cdots p_{n+m-1}$, wie c_m, c'_m, $\cdots$ aus p_0, p_1, $\cdots p_{m-1}$ zu bilden und folglich positive ganze Zahlen sind. Bemerkt man ferner, dass $\frac{a_n}{a_{n+1}}$ und $\frac{a_{n+m}}{a_{n+m+1}}$ beide in denselben rein periodischen Kettenbruch

$$(p_n;\ p_{n+1},\ \cdots\ p_{n+m-1},\ p_n,\ p_{n+1},\ \cdots\ p_{n+m-1},\ p_n,\ \cdots)$$

sich entwickeln lassen, also gleichen Werth haben, so leitet man durch Division der letzten beiden Gleichungen durch einander die folgende her:

$$C'_m \cdot A^2 + (C'_{m-1} - C_m) \cdot A - C_{m-1} = 0,$$

in welcher A für $\frac{a_n}{a_{n+1}}$ gesetzt worden ist. Diese lehrt aber den wichtigen Satz: Jeder rein periodische Kettenbruch ist die positive Wurzel einer Gleichung zweiten Grades mit ganzzahligen Coefficienten, deren zweite Wurzel negativ ist. Dieser Zusatz folgt nämlich aus dem Umstande, dass der erste und letzte Coefficient, C'_m, $-C_{m-1}$, entgegengesetzte Vorzeichen haben, das Produkt beider Wurzeln aber bekanntlich gleich $\frac{-C_{m-1}}{C'_m}$, also negativ ist.

Aus den Gleichungen (15) folgt

$$\omega = \frac{c_n A + c_{n-1}}{c'_n A + c'_{n-1}},$$

also

$$A = \frac{c_{n-1} - c'_{n-1}\omega}{c'_n\omega - c_n}.$$

Setzt man diesen Werth für A in die vorige Gleichung ein, so ergiebt sich für ω eine ähnliche quadratische Gleichung, und folglich der allgemeinere Satz: Jeder periodische Kettenbruch ist Wurzel einer quadratischen Gleichung mit ganzzahligen Coefficienten, oder, wie es früher ausgedrückt worden ist, eine quadratische Irrationelle, eine algebraische Zahl zweiten Grades.

Vierte Vorlesung.

Die quadratischen Irrationellen.

1. Der in der vorigen Vorlesung hergeleitete Satz erweckt die Frage, ob er auch umgekehrt werden darf, ob nämlich der Kettenbruch, in welchen eine (positive) Wurzel einer quadratischen Gleichung mit ganzzahligen Coefficienten entwickelt werden kann, periodisch ist oder nicht. Die Beantwortung dieser Frage steht in engster Beziehung zu der Theorie der sogenannten quadratischen Formen, insbesondere zu dem Probleme, die unbestimmte Gleichung

$$ax^2 + 2bxy + cy^2 = m, \tag{1}$$

in welcher a, b, c, m gegebene ganze Zahlen sind, in ganzen Zahlen x, y aufzulösen. Wir wollen daher zunächst hier ein paar der einfachsten Eigenschaften der quadratischen Formen, deren wir bedürfen werden, voraufschicken.

Ebenso, wie bei der Gleichung

$$a + 2bz + cz^2 = 0$$

die Zahl $D = b^2 - ac$ von Bedeutung ist, insofern ihr Vorzeichen über die Natur der Wurzeln, ob sie reell sind oder nicht, entscheidet, spielt dieselbe Zahl auch in der Theorie der quadratischen Formen eine grosse Rolle und wird deshalb die Determinante der Form genannt. Wir dürfen uns für unsern Zweck auf die Annahme beschränken, dass sie positiv und keine Quadratzahl ist.

1) Wenn man in der Form statt der Zahlen x, y zwei andere x', y' mittels der Substitution

$$x = \alpha x' + \beta y' \qquad y = \gamma x' + \delta y' \tag{2}$$

einführt, in welcher α, β, γ, δ ganze Zahlen bedeuten sollen, so geht sie in eine andere quadratische Form

$$a'x'^2 + 2b'x'y' + c'y'^2$$

mit ganzzahligen Coefficienten über, welche mit den ursprünglichen a, b, c durch nachstehende Gleichungen verbunden sind:

$$(3)\quad \begin{cases} a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 & = (a\alpha + b\gamma)\alpha + (b\alpha + c\gamma)\gamma \\ b' = (a\alpha + b\gamma)\beta + (b\alpha + c\gamma)\delta & = (a\beta + b\delta)\alpha + (b\beta + c\delta)\gamma \\ c' = a\beta^2 + 2b\beta\delta + c\delta^2 & = (a\beta + b\delta)\beta + (b\beta + c\delta)\delta. \end{cases}$$

Multiplicirt man nun die beiden Ausdrücke für b' in einander und subtrahirt davon das Produkt $a'c'$, so findet man die Beziehung

$$(4)\qquad D' = D \cdot (\alpha\delta - \beta\gamma)^2$$

zwischen den Determinanten der transformirten und der ursprünglichen Form. Hiernach werden beide Determinanten einander gleich sein, wenn der Modulus $\alpha\delta - \beta\gamma$ der Substitution (2) gleich ± 1 ist. In demselben Falle ergiebt aber die Auflösung der Gleichungen (2) die folgenden:

$$(5)\qquad \pm x' = \delta x - \beta y, \quad \pm y' = -\gamma x + \alpha y,$$

durch welche offenbar die transformirte Form rückwärts in die ursprüngliche übergeht; und es werden in diesem Falle nicht nur ganzzahligen Werthen x', y' solche für x, y entsprechen, sondern auch umgekehrt. Man nennt alsdann die beiden Formen einander äquivalent, und zwar eigentlich oder uneigentlich, je nachdem in der Gleichung

$$(6)\qquad \alpha\delta - \beta\gamma = \pm 1$$

das obere oder untere Vorzeichen zu nehmen ist; und gewinnt mit Rücksicht auf (4) den Satz: Aequivalente Formen haben gleiche Determinante.

2) Geht nun die Form $ax^2 + 2bxy + cy^2$ durch die Substitution (2) in die äquivalente Form $a'x'^2 + 2b'x'y' + c'y'^2$, desgleichen durch die Substitution

$$x = \lambda x'' + \mu y'', \quad y = \nu x'' + \varrho y''$$

in die äquivalente Form $a''x''^2 + 2b''x''y'' + c''y''^2$ über, so wird offenbar die zweite Form in diese letztere verwandelt, wenn man nach der Substitution (5) die soeben bezeichnete anwendet, d. h. durch die einzige Substitution

$$\pm x' = (\delta\lambda - \beta\nu)x'' + (\delta\mu - \beta\varrho)y''$$
$$\pm y' = (-\gamma\lambda + \alpha\nu)x'' + (-\gamma\mu + \alpha\varrho)y'',$$

welche aus ihrer Zusammensetzung hervorgeht. Da für die letztere aber ihr Modulus

$$(\delta\lambda - \beta\nu)(-\gamma\mu + \alpha\varrho) - (\delta\mu - \beta\varrho)(-\gamma\lambda + \alpha\nu)$$
$$= (\alpha\delta - \beta\gamma)\cdot(\lambda\varrho - \mu\nu)$$

also gleich ± 1 gefunden wird, je nachdem die Aequivalenzen beide gleicher oder verschiedener Art sind, so findet sich der Satz: Zwei Formen, welche einer dritten äquivalent sind, sind es auch unter einander, eigentlich oder uneigentlich, je nachdem sie der dritten Form auf gleiche oder auf verschiedene Art äquivalent sind.

3) Die Wurzeln der quadratischen Gleichung

$$a + bz + cz^2 = 0,$$

nämlich

$$z_1 = \frac{-b - \sqrt{D}}{c}, \quad z_2 = \frac{-b + \sqrt{D}}{c},$$

sollen zugleich die Wurzeln der quadratischen Form

$$ax^2 + 2bxy + cy^2$$

heissen, und zwar resp. die erste und zweite Wurzel derselben. Geht nun diese Form durch die Substitution (2) in eine äquivalente Form $a'x'^2 + 2b'x'y' + c'y'^2$ mit den Wurzeln z_1', z_2' über, so bestätigt man mit Rücksicht auf die dann stattfindenden Gleichungen (2), (4), (6) ohne Mühe die Beziehung

$$z = \frac{\gamma + \delta z'}{\alpha + \beta z'}$$

zwischen den gleichnamigen Wurzeln beider Formen, wenn die Aequivalenz eine eigentliche ist.

4) Von den Formen, welche einer gegebenen Form eigentlich äquivalent sind, heben wir für das Folgende nur diejenigen hervor, welche, wenn δ eine positive ganze Zahl bedeutet, durch die Substitution

$$(7) \qquad x = y', \quad y = -x' + \delta y'$$

daraus hervorgehen. Man findet für die Coefficienten der transformirten Form alsdann die Werthe

$$a' = c, \quad b' = -b - c\delta, \quad c' = a + 2b\delta + c\delta^2.$$

Die besondere Beziehung beider Formen zu einander besteht hiernach ausser der Aequivalenz und der aus ihr folgenden Gleichheit der Determinanten darin, dass der erste Coefficient der neuen Form gleich dem letzten der ursprünglichen Form,

und die Summe der mittleren Coefficienten durch den gemeinsamen Coefficienten theilbar ist. Zwei äquivalente Formen dieser Art sollen **benachbarte** Formen heissen, und zwar die neue der ursprünglichen **nach rechts**, diese der neuen **nach links** hin benachbart. Umgekehrt sind zwei Formen, deren Determinanten gleich sind und deren Coefficienten die angegebenen Eigenschaften haben, einander eigentlich äquivalent, und die eine geht durch eine Substitution von der Form (7), in welcher δ dem negativ genommenen Quotienten aus der Summe der mittleren und dem gemeinsamen Coefficienten gleich ist, in die andere über.

2. Wir bezeichen nun zur Abkürzung mit

$$(A_0, B_0, A_1)$$

eine quadratische Form mit den drei ganzzahligen Coefficienten A_0, B_0, A_1 und nehmen an, ihre Determinante $D = B_0^2 - A_0 A_1$ sei positiv und keine Quadratzahl, von ihren Wurzeln

$$\Omega_0 = \frac{-B_0 - \sqrt{D}}{A_1}, \quad \Omega_0' = \frac{-B_0 + \sqrt{D}}{A_1}$$

aber sei die erstere positiv. Wir können dieselbe dann, da sie irrational ist, in einen unendlichen Kettenbruch

$$\Omega_0 = (p_0; p_1, p_2, p_3, \cdots)$$

entwickeln und wollen seine Natur genauer untersuchen. Zu diesem Zwecke denken wir uns seine aufeinanderfolgenden Näherungsbrüche

$$\frac{c_0}{c_0'}, \quad \frac{c_1}{c_1'}, \quad \frac{c_2}{c_2'}, \quad \frac{c_3}{c_3'}, \quad \cdots,$$

wo also $c_0 = 1$, $c_0' = 0$, $c_1 = p_0$, $c_1' = 1$, u. s. w. ist. Transformirt man nun die Form (A_0, B_0, A_1) mittels nachstehender Substitutionen:

$$\begin{pmatrix} c_0', & c_1' \\ c_0, & c_1 \end{pmatrix}, \quad \begin{pmatrix} c_1', & c_2' \\ c_1, & c_2 \end{pmatrix}, \quad \begin{pmatrix} c_2', & c_3' \\ c_2, & c_3 \end{pmatrix}, \quad \cdots,$$

so entsteht eine Reihe anderer quadratischer Formen

$$(A_1, B_1, A_2), \; (A_2, B_2, A_3), \; (A_3, B_3, A_4), \; \cdots,$$

welche, wegen der allgemeinen Beziehung

$$c_i' c_{i+1} - c_i c_{i+1}' = (-1)^{i+1},$$

der ursprünglichen Form abwechselnd die erste uneigentlich, die zweite eigentlich, die dritte uneigentlich u. s. f. äquivalent sind. Hieraus folgen für alle Werthe $i = 0, 1, 2, 3, \cdots$ die nachstehenden Beziehungen, welche die Coefficienten der aufeinanderfolgenden Transformirten finden lehren:

$$(8)\qquad \begin{aligned} A_{i+1} &= A_0 c_i'^2 + 2B_0 c_i' c_i + A_1 c_i^2 \\ &= A_1(c_i - c_i'\Omega_0)\cdot(c_i - c_i'\Omega_0') \end{aligned}$$

$$(9)\qquad B_{i+1} = A_0 c_i' c_{i+1}' + B_0(c_i' c_{i+1} + c_i c_{i+1}') + A_1 c_i c_{i+1}$$

$$(10)\qquad B_i^2 - A_i A_{i+1} = D.$$

Nun geht offenbar eine Form $ax^2 + 2bxy + cy^2$ durch die Substitution $x = x'$, $y = -y'$, deren Modulus -1 ist, in $ax'^2 - 2bx'y' + cy'^2$ über, welche also jener Form uneigentlich äquivalent ist. Daher sind die Formen

$$(A_1, -B_1, A_2),\ (A_2, B_2, A_3),\ (A_3, -B_3, A_4),\ \cdots$$

oder allgemein die Form

$$(A_i, \varepsilon^i B_i, A_{i+1}),$$

in welcher ε statt -1 gesetzt ist, der ursprünglich gegebenen Form und folglich auch unter einander sämmtlich eigentlich äquivalent. Ersetzt man aber die Zahlen c_{i+1}, c_{i+1}' in dem obigen Ausdrucke für B_{i+1} durch ihre Werthe, nämlich $p_i c_i + c_{i-1}$, $p_i c_i' + c_{i-1}'$ resp., so findet man mit Rücksicht auf die Gleichungen (8) und (9) für jedes $i > 0$ die folgende:

$$B_{i+1} = p_i \cdot A_{i+1} + B_i,$$

der man auch die Gestalt

$$(11)\qquad \varepsilon^i \cdot B_i + \varepsilon^{i+1} \cdot B_{i+1} = \varepsilon^{i+1} p_i \cdot A_{i+1}$$

geben kann, eine Gleichung, aus welcher weiter zu schliessen ist, dass die Formen, deren eigentliche Aequivalenz wir soeben festgestellt haben, eine Reihe nach rechts hin benachbarter Formen bilden. Sie gehen daher allgemein, die i^{te} in die $(i+1)^{\text{te}}$ über durch die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & \varepsilon^i p_i \end{pmatrix}$; diese Bemerkung liefert uns aber noch die nachstehende, für jedes $i > 0$ — denn dieselbe wird nach (8) auch noch für $i = 0$ erfüllt — giltige Gleichung:

$$(12)\qquad A_{i+2} = A_{i+1} \cdot p_i^2 + 2B_i \cdot p_i + A_i.$$

3. Sehen wir jetzt, was aus diesen Beziehungen sich schliessen lässt. Im Ausdrucke (8) für A_{i+1} ist der Faktor $c_i - \Omega_0 c_i'$ nach der Natur der aufeinanderfolgenden Näherungsbrüche abwechselnd positiv und negativ, wenn i alle ganzzahligen Werthe durchläuft. Wenn daher der dritte Faktor $c_i - \Omega_0' c_i'$ von einem bestimmten Werthe des Index i an dauernd dasselbe Vorzeichen beibehält, so wird von dieser Stelle an A_{i+1} bei wachsendem Index abwechselnd das eine und das andere Vorzeichen erhalten. Dies tritt aber in der That ein. Denn, da $\frac{c_i}{c_i'} - \Omega_0$ mit wachsendem Index i gegen Null convergirt, wird es von einem hinreichend grossen Index $i = k$ an stets numerisch kleiner bleiben als $\Omega_0 - \Omega_0'$, und folglich wird dann

$$c_i - c_i'\Omega_0 + (\Omega_0 - \Omega_0')c_i' = c_i - c_i'\Omega_0'$$

dasselbe Vorzeichen haben und für jeden grösseren Werth von i behalten, wie $\Omega_0 - \Omega_0'$.

Hiernach werden

$$A_{k+1}, \quad A_{k+2}, \quad A_{k+3}, \quad \cdots$$

abwechselndes Vorzeichen haben, und es ist leicht zu sehen, dass allgemein $\varepsilon^{k+h} \cdot A_{k+h}$ positiv ist. Denn in der Formel

$$A_{k+h} = A_1 (c_{k+h-1} - c_{k+h-1}'\Omega_0)(c_{k+h-1} - c_{k+h-1}'\Omega_0')$$

hat nach der Annahme der letzte Faktor dasselbe Vorzeichen wie $\Omega_0 - \Omega_0'$, d. h. aber, da

$$\Omega_0 - \Omega_0' = \frac{2\sqrt{D}}{-A_1}$$

ist, das entgegengesetzte Vorzeichen wie A_1, und folglich muss A_{k+h} das entgegengesetzte Vorzeichen haben, wie der Ausdruck $c_{k+h-1} - c_{k+h-1}'\Omega_0$, d. h. positiv oder negativ sein, jenachdem $k + h$ gerade oder ungerade ist.

Bezeichnen hiernach Ω_{k+h}, Ω_{k+h}' die erste und zweite Wurzel der quadratischen Form

$$(A_{k+h}, \quad \varepsilon^{k+h} B_{k+h}, \quad A_{k+h+1}),$$

so sind für jedes positive h diese beiden Wurzeln nothwendig

von entgegengesetztem Vorzeichen, da A_{k+h}, A_{k+h+1} es sind. Man findet aber

$$\varepsilon^{k+h}\,\Omega_{k+h} = \frac{-B_{k+h} - \varepsilon^{k+h}\sqrt{D}}{A_{k+h+1}}$$

$$\varepsilon^{k+h+1}\cdot\Omega'_{k+h} = \frac{B_{k+h} - \varepsilon^{k+h}\sqrt{D}}{A_{k+h+1}};$$

das übereinstimmende Vorzeichen der Grössen

$$\varepsilon^{k+h}\,\Omega_{k+h}, \quad \varepsilon^{k+h+1}\,\Omega'_{k+h}$$

muss nothwendig das ihrer Summe sein und ergiebt sich so als das Vorzeichen von $\frac{-2\varepsilon^{k+h}\sqrt{D}}{A_{k+h+1}}$, d.h. von $\varepsilon^{k+h+1}A_{k+h+1}$, also als das positive.

Nun bestehen aber zwischen den gleichnamigen Wurzeln zweier aufeinanderfolgenden Formen nach No. 1, 3) die beiden Gleichungen

$$(13)\qquad \begin{cases} \Omega_{k+h-1} = \dfrac{-1-\varepsilon^{k+h}p_{k+h-1}\cdot\Omega_{k+h}}{\Omega_{k+h}} \\[2ex] \Omega'_{k+h-1} = \dfrac{-1-\varepsilon^{k+h}p_{k+h-1}\cdot\Omega'_{k+h}}{\Omega'_{k+h}}. \end{cases}$$

Schreiben wir die erste dieser Gleichungen in der Art:

$$\frac{1}{\varepsilon^{k+h}\,\Omega_{k+h}} = \varepsilon^{k+h-1}\,\Omega_{k+h-1} - p_{k+h-1},$$

so lehrt sie, dass $\varepsilon^{k+h-1}\,\Omega_{k+h-1} > p_{k+h-1}$ sein muss, gleichzeitig aber $< p_{k+h-1} + 1$; denn sonst wäre $\frac{1}{\varepsilon^{k+h}\,\Omega_{k+h}}$ grösser und folglich $\varepsilon^{k+h}\,\Omega_{k+h}$ kleiner als Eins, und es ergäbe sich, wenn man um eine Stelle weiter ginge, aus der Formel

$$\frac{1}{\varepsilon^{k+h+1}\,\Omega_{k+h+1}} = \varepsilon^{k+h}\,\Omega_{k+h} - p_{k+h},$$

in welcher jedenfalls $k+h>0$, also $p_{k+h} \geqq 1$ ist, für $\varepsilon^{k+h+1}\,\Omega_{k+h+1}$ ein negativer Werth, gegen das zuvor Bewiesene. Hieraus folgt, dass, sobald $h \geqq 1$ ist, p_{k+h-1} das grösste in $\varepsilon^{k+h-1}\,\Omega_{k+h-1}$ enthaltene Ganze ist.

Schreibt man ferner die zweite Gleichung (13) in der folgenden Form:

$$\varepsilon^{k+h}\,\Omega'_{k+h-1} = \frac{1}{\varepsilon^{k+h+1}\,\Omega'_{k+h}} - p_{k+h-1},$$

so lehrt sie zunächst für jedes $h > 1$, dass $\frac{1}{\varepsilon^{k+h+1}\Omega'_{k+h}}$ $> p_{k+h-1}$ ist. Wird aber sogar $h > 2$ vorausgesetzt, so kann $\frac{1}{\varepsilon^{k+h+1}\Omega'_{k+h}}$ nicht zugleich auch grösser sein als $p_{k+h-1} + 1$, denn sonst würde $\varepsilon^{k+h}\Omega'_{k+h-1}$ grösser, also $\frac{1}{\varepsilon^{k+h}\Omega'_{k+h-1}}$ kleiner sein als die Einheit, und wenn man um eine Stelle weiter zurückginge, würde aus der analogen Formel

$$\varepsilon^{k+h-1}\,\Omega'_{k+h-2} = \frac{1}{\varepsilon^{k+h}\,\Omega'_{k+h-1}} - p_{k+h-2}$$

gegen das zuvor Bewiesene für $\varepsilon^{k+h-1}\Omega'_{k+h-2}$ ein negativer Werth hervorgehen, da solange jedenfalls $k + h - 2 > 0$, also $p_{k+h-2} > 1$ bleibt. Für $h > 2$ ist demnach p_{k+h-1} die grösste ganze Zahl, welche in $\frac{1}{\varepsilon^{k+h+1}\Omega'_{k+h}}$ enthalten ist.

4. Nach diesen Vorbereitungen kehren wir zur Gleichung (10) zurück. Weil die Zahlen A_{k+h}, A_{k+h+1} entgegengesetzte Vorzeichen haben, sobald $h > 1$ ist, lehrt jene Gleichung, wenn man $i = k + h$ darin setzt, dass weder die Zahlen A_{k+h} die endliche Grenze D, noch die Zahlen B_{k+h} die endliche Grenze $\sqrt{D}$ überschreiten, dass mithin diesen ganzen Zahlen nur eine endliche Menge verschiedener Werthe zukommen kann. Es wird daher nothwendig geschehen müssen, dass in der fortlaufenden Reihe benachbarter Formen endlich einmal die Coefficienten einer derselben mit den Coefficienten einer früheren übereinstimmen, und zwar wird dies wegen des wechselnden Vorzeichens der äusseren Coefficienten nach einer geraden Anzahl zwischenliegender Formen eintreten müssen. Sei also, indem der Kürze wegen $k + h = n$ gesetzt wird, $A_n = A_{n+2r}$, $B_n = B_{n+2r}$, $A_{n+1} = A_{n+2r+1}$. Dann ist auch $\Omega_n = \Omega_{n+2r}$, und, da p_n, p_{n+2r} die grössten in $\varepsilon^n\Omega_n$, $\varepsilon^{n+2r}\Omega_{n+2r}$ resp. enthaltenen Ganzen sind, auch

$p_n = p_{n+2r}$. Daher folgt nun nach der Gleichung (11) $B_{n+1} = B_{n+2r+1}$, sowie endlich nach der Gleichung (12) auch $A_{n+2} = A_{n+2r+2}$, d. h. die beiden, in der Reihe äquivalenter Formen auf jene beiden bezüglich folgenden Formen sind wieder identisch; und hieraus schliesst man in Fortsetzung derselben Ueberlegungen, dass von der Form $(A_{n+2r}, \varepsilon^{n+2r} B_{n+2r}, A_{n+2r+1})$ ab die sämmtlichen auf $(A_n, \varepsilon^n B_n, A_{n+1})$ folgenden Formen sich wiederholen, dass also mit andern Worten von der Form $(A_n, \varepsilon^n B_n, A_{n+1})$ an die ganze Reihe benachbarter Formen aus einer unendlich oft wiederholten Periode von $2r$ Formen besteht. Da dasselbe alsdann bezüglich der Reihe $p_n, p_{n+1}, p_{n+2}, \cdots$ gelten muss, findet sich auf solche Weise offenbar zunächst der Satz bewiesen: Hat eine quadratische Gleichung mit ganzzahligen Coefficienten und einer Determinante, welche keine quadratische Zahl*) ist, eine positive Wurzel, so ist die Kettenbruchentwicklung dieser Wurzel periodisch — die genaue Umkehrung des am Schlusse der vorigen Vorlesung erhaltenen Ergebnisses; denn es ist von selbst einleuchtend, dass die in diesem Ergebnisse vorkommende quadratische Gleichung zur Determinante keine (positive) Quadratzahl haben kann, weil sonst die Wurzeln der Gleichung rational würden, also nur eine endliche, keine periodische d. h. unendliche Kettenbruchentwicklung zulassen würden.

Es scheint zwar, als sei im Vorigen dieser Satz nur für die erste Wurzel Ω_0 bewiesen. Indessen, wenn Ω_0' gleichfalls positiv ist, kann genau dieselbe Betrachtung auch für diese zweite Wurzel angestellt werden und führt zu demselben Ergebnisse. Die leichten Veränderungen, welche dabei eintreten, sind nur die, dass $\varepsilon^{k+h} A_{k+h}$ negativ, $\varepsilon^{k+h} \Omega_{k+h}'$, $\varepsilon^{k+h+1} \Omega_{k+h}$ positiv werden; es findet sich dagegen, dass alle weiteren Schlüsse ihre Giltigkeit behalten, wenn man durchweg die ersten und zweiten Wurzeln ihre Rolle tauschen lässt.

*) Es ist hier nicht nöthig, ausdrücklich diese Zahl als positiv vorauszusetzen, weil diese Voraussetzung schon in derjenigen einer positiven also reellen Wurzel der Gleichung mit einbegriffen ist.

5. Beachtet man weiter, dass auch $\Omega'_n = \Omega'_{n+2r}$ sein wird, so folgt, weil p_{n-1}, p_{n+2r-1} die in den Werthen $\frac{1}{\varepsilon^{n+1}\Omega'_n}$, $\frac{1}{\varepsilon^{n+2r+1}\Omega'_{n+2r}}$ bez. enthaltenen grössten Ganzen sind, auch die Gleichheit dieser beiden Zahlen, hieraus aber mittels der Beziehung (11) die Gleichheit $B_{n-1} = B_{n+2r-1}$, und endlich nach der Gleichung (12) auch $A_{n-1} = A_{n+2r-1}$, d. h. die Periode der benachbarten Formen kann auch weiter nach links hin fortgesetzt werden. Indessen ist dieser Fortsetzung eine gewisse Schranke gesetzt durch den Umstand, dass das bei dieser Überlegung benutzte Endergebniss der No. 4 nur für $h > 2$ gilt. Infolge davon wird also jedenfalls sich erschliessen lassen, dass die Periodicität in der Reihe der quadratischen Formen schon von der Form $(A_{k+2}, \varepsilon^{k+2}B_{k+2}, A_{k+3})$ und entsprechend die des Kettenbruches vom Theilnenner p_{k+2} an stattfindet. Wenn jedoch schon A_k und A_{k+1} entgegengesetztes Vorzeichen hätten, so würde, wenn $k > 0$ ist, die Fortsetzung der Periode noch um ein Glied weiter nach links hin möglich sein, diese selbst also schon mit der Form $(A_{k+1}, \varepsilon^{k+1}B_{k+1}, A_{k+2})$ bez. mit dem Theilnenner p_{k+1} ihren Anfang nehmen. Ist $k = 0$, so ist, um den gleichen Schluss ziehen zu dürfen, die Voraussetzung nothwendig, dass p_0 positiv ist. Denn er beruht wesentlich auf dem Umstande, dass p_{k+h-2} von Null verschieden ist, und dies ist für $k = 0$, $h = 2$ eben nur unter jener Voraussetzung der Fall.

6. Dies vorausgeschickt, wollen wir nun unsere bisherigen Betrachtungen specialisiren, indem wir bezüglich der Form (A_0, B_0, A_1) annehmen, nicht nur, dass die erste Wurzel Ω_0 positiv, sondern auch, dass die zweite Wurzel Ω'_0 negativ sei. Diese Annahme erfordert, dass A_0, A_1 entgegengesetzte Vorzeichen haben, nämlich A_0 positiv, A_1 negativ sei, und hat zur Folge, dass in dem Ausdrucke (8) für A_{i+1} der letzte Faktor für jeden Werth des Index i positiv ist, sodass $k = 0$ angenommen werden kann. Nach der zuletzt gemachten Vorbemerkung wird also die Periodicität des Kettenbruchs für Ω_0 sicherlich schon von dem Theilnenner p_1 an stattfinden, wenn p_0 positiv, d. h. $\Omega_0 > 1$ ist. Ist gleichzeitig Ω'_0 numerisch kleiner als Eins, so findet man aus der Beziehung

$$\varepsilon\Omega_0' = \frac{1}{\Omega_1'} - p_0,$$

dass $\frac{1}{\Omega_1'} > p_0$, aber auch $< p_0 + 1$ ist; es ergiebt sich also auch noch p_0 als die grösste in $\frac{1}{\varepsilon^2 \Omega_1'}$ enthaltene ganze Zahl, was hinreicht, um die Periodicität wieder noch einen Schritt weiter nach links zu schieben, sodass sie mit dem Anfangsgliede p_0 beginnt. So findet sich demnach der Satz: **Hat eine quadratische Gleichung mit ganzzahligen Coefficienten irrationale Wurzeln, eine positive, welche grösser als Eins, eine negative, welche kleiner als Eins ist, so ist die Kettenbruchentwicklung für die erstere rein periodisch.**

Betrachten wir insbesondere den Fall, in welchem $A_0 = 1$, $B_0 = 0$, $A_1 = -D$ ist, während wieder D positiv und von einer Quadratzahl verschieden vorausgesetzt wird, so ist $\Omega_0 = \frac{1}{\sqrt{D}}$, $\Omega_0' = \frac{-1}{\sqrt{D}}$; die besonderen Voraussetzungen, welche soeben gemacht worden sind, finden sich also erfüllt bis auf den hier verschwindenden Werth von p_0. Infolge davon wird die Kettenbruchentwicklung für Ω_0 nur von dem Theilnenner p_2 an periodisch sein; man kann aber das Ergebniss offenbar in der folgenden Weise aussprechen: **Die Quadratwurzel aus einer positiven, nicht quadratischen Zahl D kann in einen Kettenbruch**

$$(p_1; p_2, p_3, p_4, \cdots)$$

entwickelt werden, welcher von dem ersten Theilnenner an periodisch ist.

Abgesehen von den besonderen Sätzen, welche wir zuletzt ausgesprochen haben, ist das Hauptergebniss unserer Untersuchung über periodische Kettenbrüche in dem Umstande zu erblicken, dass die Eigenschaft, in einen solchen Kettenbruch entwickelt werden zu können, den durch quadratische Gleichungen bestimmten algebraischen Irrationellen charakteristisch ist, insofern diese Irrationellen solche Entwicklung zulassen, aber auch nur sie allein. Wir

haben demnach in der genannten Eigenschaft ein wichtiges *arithmetisches Kennzeichen* der quadratischen Irrationellen gefunden.

Fünfte Vorlesung.

Vorhandensein transcendenter Zahlen. — Geschichtliches über die Zahlen e und π.

1. Die Frage, ob auch für die Wurzeln von Gleichungen mit ganzzahligen Coefficienten, deren Grad höher ist als der zweite, ein ähnliches arithmetisches Kennzeichen vorhanden ist, als wir zuletzt für die quadratischen Irrationellen gefunden haben, ist, wie schon bemerkt, noch eine offene und wir lassen ihre nähere Besprechung bis auf eine spätere Stelle. Hier treten wir dagegen nun der Frage näher, ob es auch ausser den algebraischen Zahlen noch andere, ob es auch transcendente Zahlen giebt. Durch eine sehr schöne und einfache Untersuchung*), welche allein die Betrachtung der oben untersuchten Kettenbrüche erfordert, hat Liouville den strengen Nachweis geliefert, dass in der That transcendente Zahlen vorhanden sind. Das Wesentliche seiner Betrachtung ist Folgendes:

Man nennt eine Gleichung

$$(1)\quad x^n + A_1x^{n-1} + A_2x^{n-2} + \cdots + A_{n-1}x + A_n = 0$$

mit rationalen Coefficienten irreduktibel, wenn der Ausdruck n^{ten} Grades zur Linken nicht in Faktoren geringeren Grades mit gleichfalls rationalen Coefficienten zerlegbar ist. Eine solche Gleichung kann keine rationale Wurzel $\frac{p}{q}$ haben, weil sonst jener Ausdruck den rationalen Faktor $x - \frac{p}{q}$ besässe. Auch müssen alle ihre Wurzeln ungleich sein, denn andern-

*) Journal v. Liouville, Bd. 16: sur des classes très étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationelles algébriques.

falls würde bekanntlich jener Ausdruck mit dem abgeleiteten Ausdrucke

$$n x^{n-1} + (n-1) A_1 x^{n-2} + \cdots + A_{n-1} = 0$$

einen gemeinsamen, also einen rationalen Faktor haben, gegen die Voraussetzung. Durch Fortschaffen der etwa in den Coefficienten auftretenden Nenner lässt sich der Gleichung (1) diese Form geben:

$$(2) \qquad a x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0,$$

in welcher sämmtliche Coefficienten ganze Zahlen bedeuten. Wir bezeichnen ihre Wurzeln mit $x_0, x_1, x_2, \cdots x_{n-1}$, die nach dem soeben Bemerkten ungleich sind, und nehmen an, dass x_0 reell und positiv sei. Diese Zahl x_0 entwickeln wir in einen unendlichen Kettenbruch

$$x_0 = (p_0; p_1, p_2, p_3 \cdots),$$

dessen aufeinanderfolgende Näherungsbrüche

$$\frac{c_0}{c_0'}, \quad \frac{c_1}{c_1'}, \quad \frac{c_2}{c_2'}, \quad \frac{c_3}{c_3'}, \quad \ldots$$

sein mögen; diese bilden also eine rationale Zahlenreihe, welche x_0 zum Grenzwerthe hat. Der Ausdruck auf der linken Seite der Gleichung (2) kann, in Faktoren zerlegt, folgendermassen geschrieben werden:

$$a(x - x_0)(x - x_1)(x - x_2) \cdots (x - x_{n-1}),$$

und folglich erhält man, wenn für x gesetzt wird $\frac{c_i}{c_i'}$, nachfolgende Gleichung:

$$a\left(\frac{c_i}{c_i'} - x_0\right)\left(\frac{c_i}{c_i'} - x_1\right) \cdots \left(\frac{c_i}{c_i'} - x_{n-1}\right)$$
$$= \frac{a c_i^n + a_1 c_i^{n-1} c_i' + \cdots + a_{n-1} c_i c_i'^{\,n-1} + a_n c_i'^{\,n}}{c_i'^{\,n}}.$$

Der Zähler des rechtsstehenden Bruches ist jedenfalls eine gewisse ganze Zahl, welche von der Null verschieden sein muss, denn sonst hätte die irreduktible Gleichung (2) die rationale Wurzel $\frac{c_i}{c_i'}$. Wird dieselbe mit C bezeichnet, so folgt aus der vorigen Gleichung diese neue:

$$(3)\quad \frac{c_i}{c_i'} - x_0 = \frac{C}{a\,c_i'^{\,n}\left(\frac{c_i}{c_i'} - x_1\right)\left(\frac{c_i}{c_i'} - x_2\right)\cdots\left(\frac{c_i}{c_i'} - x_{n-1}\right)}.$$

Wächst nun i über jede Grenze hinaus, so nähert sich das Produkt

$$a\left(\frac{c_i}{c_i'} - x_1\right)\left(\frac{c_i}{c_i'} - x_2\right)\cdots\left(\frac{c_i}{c_i'} - x_{n-1}\right)$$

ohne Ende der endlichen, von Null verschiedenen Grenze

$$a(x_0 - x_1)(x_0 - x_2)\cdots(x_0 - x_{n-1})$$

und bleibt demnach für jedes i sicher numerisch kleiner als eine gewisse endliche Zahl k; weil zugleich C als ganze Zahl mindestens gleich ± 1 ist, wird die rechte Seite der Gleichung (3) numerisch stets grösser sein als $\frac{1}{k c_i'^{\,n}}$. Wenn man andererseits in der Gleichung (14) der 3. Vorlesung $k = i$ setzt, und versteht unter a, a_1 die Werthe x_0, 1 resp., ersetzt ferner auf ihrer rechten Seite a_1 durch seinen Ausdruck $c_i' a_i + c_{i-1}' a_{i+1}$, so nimmt mit ihrer Hilfe die linke Seite der Gleichung (3) folgende Gestalt an:

$$\frac{c_i}{c_i'} - x_0 = (-1)^i \cdot \frac{a_{i+1}}{c_i'(c_i' a_i + c_{i-1}' a_{i+1})},$$

und demnach gilt im numerischen Sinne nachstehende Ungleichheit:

$$\frac{a_{i+1}}{c_i' a_i + c_{i-1}' a_{i+1}} > \frac{1}{k \cdot c_i'^{\,n-1}},$$

aus welcher

$$c_i' \frac{a_i}{a_{i+1}} + c_{i-1}' < k \cdot c_i'^{\,n-1},$$

also umsomehr

$$\frac{a_i}{a_{i+1}} < k \cdot c_i'^{\,n-2}$$

und wieder umsomehr die Ungleichheit

$$(4)\qquad p_i < k \cdot c_i'^{\,n-2}$$

hervorgeht. Also:

Die Theilnenner eines Kettenbruches, in welchen eine positive Wurzel einer ganzzahligen irreduktibeln

algebraischen Gleichung n^{ten} Grades entwickelt werden kann, sind der Bedingung unterworfen, dass sie das Produkt aus einer gewissen endlichen Constante k in die $(n-2)^{\text{te}}$ Potenz des Nenners des nächstvorhergehenden Näherungsbruches nicht überschreiten.

2. Bildet man demnach einen Kettenbruch, für welchen die Bedingung (4) nicht erfüllbar ist, wie gross man auch die Constante k wähle, so kann der durch diesen Kettenbruch dargestellte Werth nicht die Wurzel einer irreduktibeln Gleichung n^{ten} Grades mit ganzzahligen Coefficienten sein; ebensowenig aber die Wurzel einer solchen Gleichung geringeren Grades m, denn sonst müsste ja bei einem gewissen Werthe der Constanten k die Ungleichheit $p_i < k \cdot c_i'^{\,m-2}$, umsomehr also auch die Ungleichheit (4) erfüllt sein.

Wenn endlich der Kettenbruch derartig gebildet wird, dass die Bedingung (4) nicht erfüllbar ist, wie gross man nicht allein k, sondern auch n wähle, so kann der Werth des Bruches nicht die Wurzel einer irreduktibeln Gleichung beliebig hohen Grades von der Form (2) sein, solange ihre Coefficienten ganzzahlig sind. Er kann infolge davon auch überhaupt nicht Wurzel irgend einer ganzzahligen algebraischen Gleichung von der Form (2) sein, und wäre demnach dann eine transcendente Zahl; denn hiesse die Gleichung: $f(x) = 0$, so wäre sie entweder irreduktibel, oder im entgegengesetzten Falle liesse sich der Ausdruck zur Linken in ein Produkt

$$f_1(x) \cdot f_2(x) \cdots \quad .$$

von rationalen irreduktibeln Faktoren zerlegen, und der Kettenbruch wäre dann Wurzel einer der irreduktibeln ganzzahligen Gleichungen der Form (2):

$$F_1(x) = 0, \quad F_2(x) = 0, \quad \cdots$$

welche aus der Gleichsetzung jener Faktoren mit Null und Fortschaffung der etwaigen Nenner in den Coefficienten entstehen, was er nicht sein kann.

Ein Kettenbruch von der angegebenen Beschaffenheit lässt sich aber in der That bilden. Wenn man z. B. jedesmal aus den vorhergehenden Theilnennern den folgenden p_i nach

dem Gesetze bestimmt, dass $p_i = c_i'^i$ sein soll, so wird, wie gross zunächst auch n gewählt werde, der wachsende Index i endlich $> n$ werden und dann $p_i > c_i'^2 \cdot c_i'^{n-2}$ bleiben; da aber c_i' mit wachsendem Index i über jede Grösse hinaus wächst, wird endlich, wie gross auch k gewählt werde, $c_i'^2 > k$ und $p_i > k \cdot c_i'^{n-2}$ bleiben, der Kettenbruch also auf keine Weise der Ungleichheit (4) genügen.

Hiermit ist also in völlig strenger und sehr einfacher Weise der Beweis für das Vorhandensein transcendenter Zahlen geliefert.

3. Nachdem dies aber festgestellt ist, entsteht nun eine engere Frage von dem höchsten Interesse: ob nämlich die beiden so wichtigen, überall in der höheren Analysis auftretenden Zahlen:

$$e = 2{,}7182818284 \cdots$$

$$\pi = 3{,}14159265 \cdots,$$

die Grundzahl des natürlichen Logarithmensystems und die Ludolph'sche Zahl, die den Umfang eines Kreises vom Durchmesser 1 misst, zu den algebraischen oder zu den transcendenten Zahlen gehören. Lambert*), der bekannte Berliner Akademiker aus der Zeit Friedrichs des Grossen, hat in dieser Hinsicht bereits bewiesen, dass die Zahl π wenigstens nicht rational sein könne, sowie dass die Zahl e nicht nur, sondern auch jede ihrer Potenzen mit rationalem Exponenten irrational sein müsse. Sein Beweis lässt allerdings in mehr als einer Beziehung zu wünschen, doch hat Legendre in seinen élémens de géometrie in der 4. Anmerkung, ausgehend von derselben Grundlage wie Lambert, einen einfachen Beweis von wünschenswertherer Strenge geliefert, der ihm zugleich noch das Mittel gewährte, zu zeigen, dass auch π^2 keine rationale Zahl, d. i. π nicht die Quadratwurzel aus einer solchen sein könne. Fügen wir hier hinzu, dass bezüglich der Zahl e Liouville**) etwas ähnliches, sogar umfassenderes nachgewiesen hat, nämlich, dass weder e selbst noch auch e^2

*) Lambert, mém. de l'acad. de Berlin, 1761, pag. 265.

**) Liouville's Journal de Mathématiques, t. 5, pag. 192.

Wurzel einer ganzzahligen quadratischen Gleichung sein kann, so haben wir im wesentlichen alles angeführt, was bis in die neue Zeit hinein mit Bezug auf unsere Frage geleistet worden war. Erst im Jahre 1874 gelang es Herrn Hermite, auf höchst geniale Weise und unter Anwendung höherer analytischer Hilfsmittel, den strengen Nachweis zu führen, dass die Zahl e eine transcendente Zahl ist.*) Auf seiner Grundlage weiter bauend, fand darauf Herr Lindemann**) im Jahre 1882 dasselbe Ergebniss für die Zahl π; sein nicht ganz leichter Beweis ist später von Herrn Weierstrass***) durch einfachere Betrachtungen ersetzt worden.

Obwohl hiernach die früheren Untersuchungen durch die zuletzt genannten allgemeinen Erkenntnisse überholt und überflüssig gemacht worden sind, theilen wir der Vollständigkeit wegen sie zunächst hier in der Kürze mit.

4. Die Grundlage der Untersuchungen von Lambert und Legendre ist ein gewisser unendlicher Kettenbruch, welchen wir daher zuerst herleiten müssen. Er ist zwar nicht von derselben Art, wie die in der 3. Vorlesung behandelten Kettenbrüche, doch sehen wir hier von der näheren Besprechung solcher allgemeineren Kettenbrüche und der Gesetze, denen sie unterliegen, ab, weil wir die darzustellenden Betrachtungen nicht zum Zwecke des theoretischen Aufbaues, sondern ausschliesslich ihres geschichtlichen Interesses wegen entwickeln.

Setzen wir

$$\varphi(z) = 1 + \frac{1}{z}\, y^2 + \frac{1}{z(z+1)} \frac{y^4}{1\cdot 2} + \frac{1}{z(z+1)(z+2)} \frac{y^6}{1\cdot 2\cdot 3} + \cdots,$$

so bestätigt sich ohne Mühe die Beziehung

$$\varphi(z) - \varphi(z+1) = \frac{y^2}{z(z+1)} \cdot \varphi(z+2),$$

und hieraus, wenn

$$\psi(z) = \frac{y^2}{z} \cdot \frac{\varphi(z+1)}{\varphi(z)} \tag{5}$$

*) Seine Untersuchung ist von ihm herausgegeben in der Schrift: Sur la fonction exponentielle, Paris 1874.

**) In den Mathematischen Annalen Bd. 20, pag. 213.

***) Sitzungsberichte der Berliner Akademie vom Jahre 1885, p. 1067.

gesetzt wird, folgende Gleichung:

$$\psi(z) = \frac{y^2}{z + \psi(z+1)},$$

aus welcher sogleich diese Kettenbruchentwicklung hervorgeht:

$$\psi(z) = \cfrac{y^2}{z + \cfrac{y^2}{z + 1 + \cfrac{y^2}{z + 2 + \cdots}}} \tag{6}$$

Wird nun $z = \frac{1}{2}$ und $y = \frac{x}{2}$ gewählt, so findet sich

$$\varphi(z) = 1 + \frac{x^2}{1 \cdot 2} + \frac{x^4}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots = \frac{e^x + e^{-x}}{2}$$

$$\frac{y^2}{z} \cdot \varphi(z+1) = \frac{x}{2}\left(\frac{x}{1} + \frac{x^3}{1 \cdot 2 \cdot 3} + \frac{x^5}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} + \cdots\right)$$

$$= \frac{x}{2} \cdot \frac{e^x - e^{-x}}{2}$$

und demnach aus (5) und (6) die Gleichung

$$\frac{e^x - e^{-x}}{e^x + e^{-x}} = \cfrac{\frac{x}{2}}{\frac{1}{2} + \cfrac{\frac{x^2}{4}}{\frac{3}{2} + \cfrac{\frac{x^2}{4}}{\frac{5}{2} + \cdots}}} = \cfrac{x}{1 + \cfrac{x^2}{3 + \cfrac{x^2}{5 + \cdots}}} \tag{7}$$

Aus dieser Gleichung geht durch den Übergang zum Imaginären, indem nämlich x verwandelt wird in $x\sqrt{-1}$ — ein Verfahren, dessen Zulässigkeit freilich erst gerechtfertigt werden müsste — mit Hilfe der bekannten Formel der Analysis

$$\operatorname{tang} x = \frac{1}{i} \frac{e^{xi} - e^{-xi}}{e^{xi} + e^{-xi}}$$

worin $i = \sqrt{-1}$, die neue Gleichung hervor:

$$\operatorname{tang} x = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cdots}}} \tag{8}$$

Dies sind die beiden von Lambert gegebenen Kettenbrüche, an welche wir nun anzuknüpfen haben.

5. Betrachten wir nämlich einen unendlichen Kettenbruch

$$(9)\qquad \cfrac{m}{n+\cfrac{m'}{n'+\cfrac{m''}{n''+\cfrac{m'''}{n'''+\cdots}}}}$$

in welchem sowohl die einzelnen Zähler $m, m', m'', \cdots$ als auch die einzelnen Nenner $n, n', n'', \cdots$ ganze Zahlen sind, deren letztere offenbar, indem man den jedesmaligen Zähler mit passendem Vorzeichen nimmt, positiv vorausgesetzt werden dürfen, so wird der Werth des Kettenbruchs wesentlich irrational sein müssen, sobald die einzelnen Brüche $\frac{m}{n}, \frac{m'}{n'}, \frac{m''}{n''}, \cdots$ numerisch kleiner sind als Eins.

Um sich hiervon zu überzeugen, bemerke man zunächst, dass der Kettenbruch keinenfalls grösser als Eins werden kann. Denn, da $\frac{m}{n}$ numerisch kleiner als Eins sein soll, so ist der numerische Werth von m kleiner als $n-1$; $n+\frac{m'}{n'}$ aber ist sicher $> n-1$, also $\frac{m}{n+\frac{m'}{n'}}$ numerisch kleiner als Eins. Dasselbe gilt aus ähnlichen Gründen von dem Bruche $\frac{m'}{n'+\frac{m''}{n''}}$; folglich ist $n+\frac{m'}{n'+\frac{m''}{n''}}$ grösser als $n-1$ und demnach $\cfrac{m}{n+\cfrac{m'}{n'+\cfrac{m''}{n''}}}$ numerisch unter der Einheit, u. s. f.; wie weit der Kettenbruch auch fortgesetzt werde, er wird niemals die Einheit übertreffen. Das Gleiche wird aber auch von denjenigen Kettenbrüchen gelten, welche aus dem vorigen hervorgehn, wenn man einen oder mehrere der Brüche am Anfange desselben unterdrückt.

Auch der Einheit gleich sein kann der ins Unendliche fortgesetzte Kettenbruch, resp. die letztgenannten Theile des-

selben, nur in einem einzigen Falle. Soll nämlich, wo zur Abkürzung ω für den Kettenbruch

$$\cfrac{m'}{n' + \cfrac{m''}{n'' + \cfrac{m'''}{n''' + \cdots}}}$$

steht, $\frac{m}{n+\omega} = \pm 1$ oder $\frac{\pm m}{n+\omega} = 1$ sein, so folgt aus $\pm m = n + \omega$ nothwendig, dass $\omega = -1$ also $n = \pm m + 1$ sei; dann müsste, unter ω' den Kettenbruch

$$\cfrac{m''}{n'' + \cfrac{m'''}{n''' + \cdots}}$$

verstanden, $\frac{m'}{n' + \omega'} = -1$, $m' = -n' - \omega'$ sein. Hieraus folgt aber nothwendig $\omega' = -1$ also $n' = -m' + 1$ u. s. f., sodass der Kettenbruch ω nur dann die Einheit zum Grenzwerthe haben kann, wenn er die Gestalt hat:

$$\cfrac{m}{\pm m + 1 + \cfrac{m'}{-m' + 1 + \cfrac{m''}{-m'' + 1 + m''' \cdots}}}$$

Da jedoch die Kettenbrüche, welche wir hier zu betrachten haben werden, diese Gestalt nicht besitzen, dürfen wir von diesem Ausnahmefalle absehn und dann sagen: Der Kettenbruch (9) und die daraus durch Unterdrückung von 1, 2, 3, $\cdots$ Brüchen am Anfange hergeleiteten Kettenbrüche sind **sämmtlich numerisch kleiner als Eins.**

Wollte man nun gegen die Behauptung des Satzes annehmen, der Kettenbruch (9) sei rational, nämlich gleich $\frac{b}{a}$:

$$\frac{b}{a} = \cfrac{m}{n + \cfrac{m'}{n' + \cfrac{m''}{n'' + \cdots}}}$$

so bestimme man Werthe c, d, e, $\cdots$ durch nachstehende Gleichungen:

$$\frac{c}{b} = \cfrac{m'}{n' + \cfrac{m''}{n'' + \cfrac{m'''}{n''' + \cdots}}}$$

$$\frac{d}{c} = \cfrac{m''}{n'' + \cfrac{m'''}{n''' + \cdots}}$$

u. s. w. Dem eben Gesagten zufolge bilden die Werthe b, c, d, e, $\cdots$ eine unbegrenzte Reihe abnehmender Werthe. Ferner aber finden sich aus den Gleichungen

$$\frac{b}{a} = \frac{m}{n + \frac{c}{b}}, \quad \frac{c}{b} = \frac{m'}{n' + \frac{d}{c}} \quad \text{u. s. w.}$$

die folgenden:

$$c = ma - nb, \quad d = m'b - n'c, \quad e = m''c - n''d, \quad \cdots$$

aus welchen sich c, d, e, $\cdots$ als ganze Zahlen ergeben. Man gelangt also zu einer unbegrenzten Reihe numerisch abnehmender ganzzahliger Werthe, welche nicht möglich ist, und damit ist die Behauptung erwiesen.

Dieselbe Behauptung bleibt auch richtig, wenn der Kettenbruch (9) nicht vom Anfange, sondern erst von einer späteren Stelle an die Bedingungen des vorigen Satzes erfüllt. Erfüllt er sie z. B. erst vom Gliede $\frac{m'''}{n'''}$ an, so würde der Kettenbruch

$$\omega = \cfrac{m'''}{n''' + \cfrac{m''''}{n'''' + \cdots}}$$

nach dem vorigen Satze irrational sein, und daher auch, wie leicht zu sehen, der Bruch

$$\cfrac{m}{n + \cfrac{m'}{n' + \cfrac{m''}{n'' + \omega}}}$$

d. h. der ganze Kettenbruch (9), nicht rational sein können.

6. Nachdem diese Hilfsbetrachtung zu Ende geführt ist, wollen wir nun annehmen, in den Kettenbrüchen (7) und (8) werde unter x ein rationaler Werth $\frac{p}{q}$ verstanden. Sie werden

dann offenbar von einer gewissen Stelle an die Bedingungen des Hilfssatzes erfüllen, da die Brüche

$$\frac{p^2}{1\cdot q^2},\quad \frac{p^2}{3\cdot q^2},\quad \frac{p^2}{5\cdot q^2},\quad \ldots$$

von einer bestimmten Stelle an kleiner als Eins bleiben. Hieraus schliessen wir dann also sogleich, dass weder e^x noch $\operatorname{tang} x$ gleichzeitig mit x rational sein können, oder anders ausgedrückt: *Jede Potenz von e mit rationalem Exponenten ist irrational. Desgleichen ist die Tangente jedes rationalen Bogens irrational.*

Da nun für $x = \frac{\pi}{4}$ gefunden wird $\operatorname{tang} x = \operatorname{tang}\frac{\pi}{4} = 1$ also gleich einer rationalen Zahl, so kann $\frac{\pi}{4}$ und folglich auch π nicht einer rationalen Zahl gleich sein. Wir schliessen demnach: *Die Zahl π ist irrational.*

Diesen *Lambert*'schen Sätzen konnte *Legendre*, wie schon bemerkt, vermittelst seines Hilfssatzes noch einen weiteren hinzufügen. Die Gleichung (8) giebt nämlich, wenn $x = \pi$ gesetzt wird, die folgende:

$$0 = \cfrac{\pi}{1 - \cfrac{\pi^2}{3 - \cfrac{\pi^2}{5 - \cdots}}}$$

welche nicht anders bestehen kann, als wenn der die Zahl π theilende Ausdruck unendlich gross und folglich

$$3 - \cfrac{\pi^2}{5 - \cfrac{\pi^2}{7 - \cdots}} = 0$$

ist. *Demnach kann π^2 keine rationale Zahl sein*, denn sonst wäre der Kettenbruch von der Art des Kettenbruches (9) und könnte demnach nicht den rationalen Werth 0 haben, den er doch besitzt.

7. Die Irrationalität der Zahl e selbst kann übrigens weit einfacher mittels der bekannten, diese Zahl definirenden Reihe

$$e = 2 + \frac{1}{1\cdot 2} + \frac{1}{1\cdot 2\cdot 3} + \frac{1}{1\cdot 2\cdot 3\cdot 4} + \cdots$$

nachgewiesen werden; doch scheint dieselbe nicht geeignet, um auch das allgemeinere Ergebniss von Lambert daraus zu gewinnen. Dagegen hat Liouville sie benutzt, um zu zeigen, dass weder e selbst, noch auch e^2 Wurzel einer ganzzahligen quadratischen Gleichung sein kann.

Aus der Reihe

$$e^x = 1 + \frac{x}{1} + \frac{x^2}{1 \cdot 2} + \frac{x^3}{1 \cdot 2 \cdot 3} + \cdots$$

findet man zunächst ohne Mühe, wenn man sie nicht ins Unendliche fortsetzt, sondern nach der n^{ten} Potenz abbricht, folgende Gleichung:

$$(10)\quad \begin{aligned} e^x = 1 + \frac{x}{1} + \frac{x^2}{1 \cdot 2} + \cdots + \frac{x^m}{1 \cdot 2 \cdot 3 \cdots m} + \cdots + \frac{x^n}{1 \cdot 2 \cdot 3 \cdots n} \\ + \frac{x^n}{1 \cdot 2 \cdot 3 \cdots n} \cdot \frac{\Theta x}{n + 1 - x}, \end{aligned}$$

in welcher Θ einen positiven echten Bruch bezeichnet. Für $x = 1$ liefert diese Formel den Werth von e unter der Form:

$$(11)\quad \begin{aligned} e = 2 + \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 2 \cdot 3} + \cdots + \frac{1}{1 \cdot 2 \cdot 3 \cdots m} + \cdots + \frac{1}{1 \cdot 2 \cdot 3 \cdots n} \\ + \frac{1}{1 \cdot 2 \cdot 3 \cdots n} \cdot \frac{\Theta}{n}, \end{aligned}$$

wobei n eine beliebig grosse Zahl bedeutet. Wäre demnach e eine rationale Zahl, so dürfte man unter n auch den Nenner des möglichst gekürzten Bruches $e = \frac{m}{n}$ verstehen, und erhielte sodann aus der vorigen Gleichung, indem man sie mit $1 \cdot 2 \cdot 3 \cdots n$ multiplicirt und die so entstehenden ganzzahligen Bestandtheile sämmtlich nach links schafft, eine Gleichung von der Form: $N = \frac{\Theta}{n}$, in welcher links eine ganze Zahl N, rechts aber ein echter Bruch steht, was widersinnig ist. Die Zahl e ist daher jedenfalls irrational.

Nun setze man ferner in (10) $x = -1$ und bezeichne -1 mit ε, so kommt

$$(12)\quad \begin{aligned} e^{-1} = 1 + \varepsilon + \frac{\varepsilon^2}{1 \cdot 2} + \cdots + \frac{\varepsilon^n}{1 \cdot 2 \cdot 3 \cdots n} \\ + \frac{\varepsilon^{n+1}}{1 \cdot 2 \cdot 3 \cdots n} \cdot \frac{\Theta'}{n + 2}, \end{aligned}$$

wobei wieder Θ' einen positiven echten Bruch bezeichnet, welcher aber mit Θ in der Gleichung (11) nicht dasselbe zu sein braucht. Nehmen wir nun an, e sei Wurzel einer quadratischen Gleichung

$$ax^2 - bx + c = 0$$

mit ganzzahligen Coefficienten a, b, c, so dürfen wir zuvörderst den ersten der Coefficienten als positiv voraussetzen, und müssten dann also

$$ae^2 - be + e = 0$$

oder auch

$$ae + ce^{-1} = b$$

haben, eine Gleichung, welche nach Einsetzung der Reihen (11) und (12) für e und e^{-1} folgende Gestalt erhält:

$$a\left(1 + 1 + \frac{1}{1 \cdot 2} + \cdots + \frac{1}{1 \cdot 2 \cdot 3 \cdots n}\right)$$
$$+ c\left(1 + \varepsilon + \frac{\varepsilon^2}{1 \cdot 2} + \cdots + \frac{\varepsilon^n}{1 \cdot 2 \cdot 3 \cdots n}\right)$$
$$+ a \cdot \frac{1}{1 \cdot 2 \cdot 3 \cdots n} \cdot \frac{\Theta}{n} + c \cdot \frac{\varepsilon^{n+1}}{1 \cdot 2 \cdot 3 \cdots n} \cdot \frac{\Theta'}{n+2} = b.$$

Hieraus folgt aber durch Multiplikation mit $1 \cdot 2 \cdot 3 \cdots n$ und, wenn die ganzzahligen Bestandtheile darauf nach rechts geschafft werden,

$$a \cdot \frac{\Theta}{n} + c\varepsilon^{n+1} \cdot \frac{\Theta'}{n+2} = N,$$

unter N eine gewisse ganze Zahl verstanden. Nun liess sich n zunächst so wählen, dass $c\varepsilon^{n+1}$ positiv wird. Hierzu ist ja nur nöthig, n gerade oder ungerade zu wählen, jenachdem c negativ oder positiv ist. Ferner aber gilt unsere Betrachtung, wie grofs diese so gewählte Zahl n auch sei; mit wachsendem n wird aber endlich der positive Ausdruck links kleiner als die Einheit, während die Zahl N rechts immer eine ganze Zahl bleibt; dies ist ein Widerspruch und folglich kann e nicht Wurzel einer quadratischen Gleichung mit ganzzahligen Coefficienten sein.

Dasselbe gilt nun aber auch für e^2. Um dies zu erweisen, erinnern wir zuerst an eine bekannte Formel der Zahlentheorie. Bezeichnet $E(x)$ das grösste Ganze, welches in

dem positiven Werthe x enthalten ist, und m eine positive ganze Zahl, so giebt die Summe

$$E\left(\frac{m}{2}\right) + E\left(\frac{m}{4}\right) + E\left(\frac{m}{8}\right) + \cdots,$$

fortgesetzt, bis sie von selber abbricht, die Anzahl an, wie oft der Faktor 2 in dem Produkte $1 \cdot 2 \cdot 3 \cdots m$ enthalten ist. Insbesondere findet sich hiernach, wenn $m = 2^i$ ist, der Werth jener Summe oder diese Anzahl gleich

$$2^{i-1} + 2^{i-2} + \cdots + 2 + 1$$

d. i. $2^i - 1$ d. i.

$$m - 1,$$

und wenn $m = 2^i + 1$ ist, gleich $2^i - 1$ d. i.

$$m - 2.$$

Allgemein aber ist jene Summe selbstverständlich kleiner als die unendliche Reihe

$$\frac{m}{2} + \frac{m}{4} + \frac{m}{8} + \cdots,$$

deren Werth m ist. Hebt man demnach im Bruche

$$\frac{2^m}{1 \cdot 2 \cdot 3 \cdots m}$$

nach Möglichkeit den Faktor 2 aus Zähler und Nenner heraus, so bleibt im Zähler eine Potenz von 2, etwa 2^{α_m} mit positivem Exponenten α_m, welcher speciell in den beiden hervorgehobenen Fällen den Werth 1 bez. 2 haben wird; der so vereinfachte Bruch möge $\frac{2^{\alpha_m}}{p_m}$ genannt werden. Ist $n > m$ und setzt man, in gleicher Weise vereinfacht,

$$\frac{2^n}{1 \cdot 2 \cdot 3 \cdots n} = \frac{2^{\alpha_n}}{p_n},$$

so wird der Nenner p_n offenbar alle in p_m verbliebenen, nämlich ungeraden Faktoren ebenfalls enthalten, also durch p_m theilbar sein müssen.

Dies vorausgeschickt, wollen wir nun die Annahme untersuchen, dass e^2 Wurzel der Gleichung

$$ax^2 - bx + c = 0$$

mit ganzzahligen Coefficienten sei. Man müsste dann

$$ae^2 + ce^{-2} = b$$

haben, oder nach Einsetzen der Werthe von e^2 und e^{-2}, nämlich

$$e^2 = 1 + \frac{2}{1} + \cdots + \frac{2^m}{1 \cdot 2 \cdot 3 \cdots m} + \cdots + \frac{2^n}{1 \cdot 2 \cdot 3 \cdots n}$$

$$+ \frac{2^n}{1 \cdot 2 \cdot 3 \cdots n} \cdot \frac{2\Theta}{n-1}$$

oder

$$e^{+2} = 1 + \frac{2}{1} + \cdots + \frac{2^{\alpha_m}}{p_m} + \cdots + \frac{2^{\alpha_n}}{p_n} + \frac{2^{\alpha_n}}{p_n} \cdot \frac{2\Theta}{n-1}$$

und

$$e^{-2} = 1 + \frac{2\varepsilon}{1} + \cdots + \frac{2^{\alpha_m} \cdot \varepsilon^m}{p_m} + \cdots + \frac{2^{\alpha_n}\varepsilon^n}{p_n}$$

$$+ \frac{2^{\alpha_n}\varepsilon^{n+1}}{p_n} \cdot \frac{2\Theta'}{n+3},$$

folgende Gleichung:

$$a\left(1 + \frac{2}{1} + \cdots + \frac{2^{\alpha_m}}{p_m} + \cdots + \frac{2^{\alpha_n}}{p_n}\right)$$

$$+ c\left(1 + \frac{2\varepsilon}{1} + \cdots + \frac{2^{\alpha_m}\varepsilon^m}{p_m} + \cdots + \frac{2^{\alpha_n}\varepsilon^n}{p_n}\right)$$

$$+ a \cdot \frac{2^{\alpha_n}}{p_n} \cdot \frac{2\Theta}{n-1} + c \cdot \frac{2^{\alpha_n}\varepsilon^{n+1}}{p_n} \cdot \frac{2\Theta'}{n+3} = b.$$

Multiplicirt man diese Gleichung mit p_n, so werden alle Glieder der in a und in c multiplicirten Klammern ganze Zahlen, und wenn man dann alle ganzzahligen Bestandtheile nach rechts schafft, entsteht folgende Gleichung:

$$a \cdot 2^{\alpha_n} \cdot \frac{2\Theta}{n-1} + c \cdot 2^{\alpha_n} \cdot \varepsilon^{n+1} \cdot \frac{2\Theta'}{n+3} = N, \tag{13}$$

unter N eine gewisse ganze Zahl verstanden. Wir dürfen hierbei wieder unter n eine gerade oder ungerade Zahl verstehen, jenachdem c negativ oder positiv ist, wodurch alsdann die beiden Glieder zur Linken wesentlich positiv werden. Dies mag z. B. in der Weise bewirkt werden, dass wir $n = 2^i$ wählen, wenn c negativ, $n = 2^i + 1$, wenn c positiv ist. Dem entsprechend würde dann der Werth der linken Seite durch den Ausdruck

$$(14)\quad 4\left(\frac{a\Theta}{n-1}+\frac{c\varepsilon^{n+1}\cdot\Theta'}{n+3}\right)\ \text{resp.}\ 8\left(\frac{a\Theta}{n-1}+\frac{c\varepsilon^{n+1}\Theta'}{n+3}\right)$$

gegeben. Wir dürfen aber endlich bei unserer Betrachtung das so gewählte n beliebig gross annehmen, und werden dies bei der bereits getroffenen Wahl von n in beiden Fällen einfach dadurch erreichen, dass wir den Exponenten i hinreichend gross wählen. Da hierbei mit dem unendlich wachsenden n die Ausdrücke (14) unendlich abnehmen werden, sinken sie schliesslich, ohne Null zu sein, unter die Einheit herab, während N eine ganze Zahl bleibt. Die Gleichung (13) ergiebt dann einen Widerspruch, und folglich ist damit der Beweis der Behauptung erbracht.

Sechste Vorlesung.

Hermite's Untersuchung der Zahl e.

1. Die in der vorigen Vorlesung entwickelten, die Zahlen e und π betreffenden Sätze sind nur ganz besondere Fälle des allgemeinen Ergebnisses, welches für die Zahl e von Hermite*), für die Zahl π von Lindemann festgestellt worden ist, dass nämlich jede dieser beiden Zahlen eine transcendente Zahl ist. Wir werden zunächst hier versuchen, von den Hermite'schen Betrachtungen, welche auch denen von Lindemann zum Grunde liegen, eine zusammenhängende Darstellung zu geben.

Versteht man unter A die Funktion $\sin x$ oder in bekannter Reihenform

$$A=\frac{x}{1}-\frac{x^3}{1\cdot 2\cdot 3}+\frac{x^5}{1\cdot 2\cdot 3\cdot 4\cdot 5}-\cdots,$$

kürzer, mit Anwendung des Summenzeichens,

*) Ausser der schon genannten Schrift Sur la fonction exponentielle kommen hier auch noch in Betracht die beiden kleinen Abhandlungen im Journal f. d. r. u. a. Mathematik Bd. 76 pag. 303 u. 342.

$$(1)\qquad A = \sum_{k=0}^{k=\infty} \frac{(-1)^k\, x^{2k+1}}{1\cdot 2\cdot 3\cdots(2k+1)}$$

und bildet hieraus die unbegrenzte Reihe von Grössen A_1, A_2, A_3, $\cdots$ nach dem Gesetze, welches die Formeln ausdrücken:

$$A_1 = \int_0^x x A\, dx, \quad A_2 = \int_0^x x A_1\, dx, \quad \cdots$$

allgemein

$$(2)\qquad A_n = \int_0^x x A_{n-1}\, dx,$$

so findet sich vermittelst der für A gegebenen Reihenentwicklung (1) ohne Mühe

$$(3)\quad A_n = x^{2n+1}\cdot \sum_{k=0}^{\infty} \frac{(-1)^k}{1\cdot 2\cdot 3\cdots 2k}\cdot \frac{x^{2k}}{(2k+1)(2k+3)\cdots(2k+2n+1)}.$$

Wird andererseits $\mathfrak{A} = \frac{\sin x}{x}$ gesetzt und hieraus die Reihe der Grössen $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$, $\cdots$ durch die Gleichungen

$$\mathfrak{A}_1 = -\frac{1}{x}\frac{d\mathfrak{A}}{dx}, \quad \mathfrak{A}_2 = -\frac{1}{x}\frac{d\mathfrak{A}_1}{dx}, \quad \cdots$$

allgemein

$$(4)\qquad \mathfrak{A}_n = -\frac{1}{x}\frac{d\mathfrak{A}_{n-1}}{dx}$$

hergeleitet, so ergiebt sich gleichfalls unschwer

$$(5)\quad \mathfrak{A}_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)(2k+3)\cdots(2k+2n+1)}\cdot \frac{x^{2k}}{1\cdot 2\cdot 3\cdots 2k},$$

d. h. es ist

$$(6)\qquad \mathfrak{A}_n = \frac{A_n}{x^{2n+1}},$$

folglich auch

$$(7)\qquad \mathfrak{A}_{n+1} = \frac{A_{n+1}}{x^{2n+3}}.$$

Wird nun in (4) $n+1$ statt n, darauf die Werthe (6) und (7) eingesetzt und die aus der Definitionsgleichung (2) hervorgehende Beziehung

$$\frac{dA_n}{dx} = x A_{n-1}$$

beachtet, so findet sich folgende interessante Recursionsformel:

$$(8) \qquad A_{n+1} = (2n+1) A_n - x^2 \cdot A_{n-1}.$$

Die hieraus für $n = 1, 2, 3, \cdots$ entstehenden Gleichungen:

$$A_2 = 3A_1 - x^2 A$$

$$A_3 = 5A_2 - x^2 A_1$$

$$A_4 = 7A_3 - x^2 A_2$$

$$\cdots\cdots\cdots$$

können folgendermassen geschrieben werden:

$$\frac{x^2 A}{A_1} = 3 - \cfrac{x^2}{\cfrac{x^2 A_1}{A_2}}$$

$$\frac{x^2 A_1}{A_2} = 5 - \cfrac{x^2}{\cfrac{x^2 A_2}{A_3}}$$

$$\frac{x^2 A_2}{A_3} = 7 - \cfrac{x^2}{\cfrac{x^2 A_3}{A_4}}$$

$$\cdots\cdots\cdots$$

und liefern daher durch allmähliches Einsetzen den Kettenbruch

$$\frac{x^2 A}{A_1} = 3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \cdots}}.$$

Aber aus $A = \sin x$ folgt sogleich

$$A_1 = \int_0^x x A\, dx = \sin x - x \cos x,$$

folglich ist

$$\frac{\sin x - x\cos x}{\sin x} = \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \cdots}}}$$

und hieraus

$$\operatorname{tang} x = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \cdots}}}}$$

So sind wir zunächst auf anderem Wege zu dem Kettenbruche zurückgeführt worden, welchen für $\operatorname{tang} x$ schon Lambert angegeben hatte.

2. Aber wir wollen uns nun genauer mit dem Ausdrucke A_n beschäftigen. Man kann statt desselben einen zweiten von ganz anderer Gestalt aufstellen, wenn man die Integrationen in den Definitionsgleichungen ohne die Reihenentwicklung für $\sin x$, mit Anwendung vielmehr der partiellen Integration ausführt. Man findet so zunächst

$$A_1 = \int_0^x x \sin x\, dx = \sin x - x \cos x$$

$$A_2 = \int_0^x x A_1\, dx = (3 - x^2) \sin x - 3x \cos x$$

$$A_3 = \int_0^x x A_2\, dx = (15 - 6x^2) \sin x - (15x - x^3) \cos x$$

u. s. w. Es stellt sich hiernach für A_n die allgemeine Form heraus:

$$A_n = \psi(x) \cdot \sin x + \chi(x) \cdot \cos x, \tag{9}$$

wo $\psi(x)$ eine gerade ganze Funktion vom n^{ten} bez. $(n-1)^{\text{ten}}$ Grade ist, jenachdem n gerade oder ungerade, $\chi(x)$ eine ungerade ganze Funktion vom $(n-1)^{\text{ten}}$ oder n^{ten} Grade je nach den beiden unterschiedenen Fällen ist; die Coefficienten dieser Funktionen sind ganze Zahlen. Wir wollen vor allen Dingen das Induktionsgesetz bestätigen.

Dazu bemerken wir zuerst die leicht durch partielle Integration zu erhaltenden Formeln

$$\int \varphi(x) \sin x\, dx = \sin x \cdot \Phi'(x) - \cos x \cdot \Phi(x)$$

$$\int \varphi(x) \cos x\, dx = \sin x \cdot \Phi(x) + \cos x \cdot \Phi'(x),$$

in welchen zur Abkürzung

$$\Phi(x) = \varphi(x) - \varphi''(x) + \varphi^{(4)}(x) - \cdots$$

gesetzt ist. Die Funktionen $\Phi(x)$, $\Phi'(x)$ in diesen Formeln sind ganze Funktionen von gleichem, bezw. um 1 geringeren Grade wie die Funktion $\varphi(x)$. Bei der Integration von 0 bis x giebt die erste Formel die folgende:

$$\int_0^x \varphi(x) \sin x\, dx = \sin x \cdot \Phi'(x) - \cos x \cdot \Phi(x) + \Phi(0),$$

also, so oft $\Phi(0)$ Null ist, was z. B. eintrifft, wenn $\varphi(x)$ und folglich seine Ableitungen gerader Ordnung also auch $\Phi(x)$ ungerade Funktionen von x sind,

$$(10) \qquad \int_0^x \varphi(x) \sin x\, dx = \sin x \cdot \Phi'(x) - \cos x \cdot \Phi(x).$$

Ebenso ergiebt die zweite Formel, wenn $\varphi(x)$ und folglich seine Ableitungen gerader Ordnung gerade Funktionen, $\Phi'(x)$ also eine ungerade Funktion von x ist,

$$(11) \qquad \int_0^x \varphi(x) \cos x\, dx = \sin x \cdot \Phi(x) + \cos x \cdot \Phi'(x).$$

Nehmen wir nunmehr an, das für A_n ausgesprochene Gesetz sei bis zu einem bestimmten Index n hin bestätigt, so würde sich finden

$$A_{n+1} = \int_0^x x A_n\, dx = \int_0^x (x\psi(x) \sin x + x\chi(x) \cos x)\, dx.$$

Ist nun zuerst n eine gerade Zahl, so wäre $\psi(x)$ eine gerade Funktion vom n^{ten}, demnach $x\psi(x)$ eine ungerade Funktion vom $(n+1)^{\text{ten}}$ Grade, und $\chi(x)$ eine ungerade Funktion $(n-1)^{\text{ten}}$, demnach $x\chi(x)$ eine gerade Funktion n^{ten} Grades. In Anwendung der Hilfsformeln (10) und (11) erhielte man also zwei Gleichungen von der Form

$$\int_0^x x\psi(x) \sin x\, dx = \sin x \cdot \Psi'(x) - \cos x \cdot \Psi(x)$$

$$\int_0^x x\chi(x) \cos x\, dx = \sin x \cdot X(x) + \cos x \cdot X'(x);$$

$\Psi(x)$, $X(x)$ bedeuten dabei, was aus $\Phi(x)$ entsteht, wenn bezw. $x\psi(x)$ und $x\chi(x)$ für $\varphi(x)$ gesetzt werden. $\Psi(x)$ muss daher eine ganzzahlige ungerade Funktion $(n+1)^{\text{ten}}$ und demnach $\Psi'(x)$ eine gerade Funktion n^{ten} Grades, $X(x)$ eine ganzzahlige gerade Funktion n^{ten} Grades, demnach $X'(x)$ eine ungerade Funktion $(n-1)^{\text{ten}}$ Grades sein. Zieht man daher zusammen:

$$A_{n+1} = \sin x \cdot \big(\Psi'(x) + X(x)\big) - \cos x \cdot \big(\Psi(x) - X(x)\big),$$

so ist nun, wo der Index $n+1$ eine ungerade Zahl ist, der $\sin x$ in eine gerade Funktion n^{ten}, der $\cos x$ in eine ungerade Funktion $(n+1)^{\text{ten}}$ Grades multiplicirt, das Induktionsgesetz also um einen Schritt weiter bestätigt. Da dasselbe Verfahren auch in dem Falle eines ungeraden n anwendbar ist und zum Ziele führt, ist also der allgemeine Nachweis geführt, dass das bezüglich A_n aufgestellte Gesetz ohne Ausnahme giltig ist.

3. Nun kann man leicht den ersten Ausdruck (3) für A_n in die Gestalt eines bestimmten Integrales überführen. In der That giebt die partielle Integration zunächst folgende Reduktionsformel:

$$(12)\quad \int_0^1 (1-z^2)^n \cdot z^{2k} dz = \frac{2k-1}{2n+2k+1} \cdot \int_0^1 (1-z^2)^n \cdot z^{2(k-1)} dz,$$

durch deren wiederholte Anwendung die Gleichung hervorgeht:

$$(13)\quad \begin{aligned} &\int_0^1 (1-z^2)^n \cdot z^{2k} dz \\ &= \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{(2n+3)(2n+5)\cdots(2n+2k+1)} \cdot \int_0^1 (1-z^2)^n dz. \end{aligned}$$

Es ist aber

$$\int_0^1 (1-z^2)^n dz = \int_0^1 (1-z^2)^{n-1} dz - \int_0^1 z^2 (1-z^2)^{n-1} dz,$$

und die Hilfsformel (12) liefert, wenn darin $n-1$ statt n und $k=1$ gesetzt wird,

$$\int_0^1 z^2 (1-z^2)^{n-1} dz = \frac{1}{2n+1} \cdot \int_0^1 (1-z^2)^{n-1} dz;$$

hiernach geht die vorige Gleichung über in

$$\int_0^1 (1-z^2)^n dz = \frac{2n}{2n+1} \cdot \int_0^1 (1-z^2)^{n-1} dz$$

und durch wiederholte Anwendung dieser Formel in

$$\int_0^1 (1-z^2)^n dz = \frac{2 \cdot 4 \cdot 6 \cdots 2n}{3 \cdot 5 \cdot 7 \cdots (2n+1)}.$$

Demnach erhält man die Formel (13) in folgender Gestalt:

$$(14) \quad \int_0^1 (1-z^2)^n \cdot z^{2k} dz = \frac{1 \cdot 3 \cdot 5 \cdots (2k-1) \cdot 2 \cdot 4 \cdot 6 \cdots 2n}{1 \cdot 3 \cdot 5 \cdot 7 \cdots (2n+2k+1)}.$$

Betrachten wir nun das Integral

$$\int_0^1 (1-z^2)^n \cdot \cos xz \, dz$$

und ersetzen darin $\cos xz$ durch seine bekannte Reihe

$$1 - \frac{x^2 z^2}{1 \cdot 2} + \frac{x^4 z^4}{1 \cdot 2 \cdot 3 \cdot 4} - \frac{x^6 z^6}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} + \cdots$$

oder kürzer, mit Anwendung des Summenzeichens,

$$\cos xz = \sum_0^\infty {}_k \frac{(-1)^k \cdot x^{2k} z^{2k}}{1 \cdot 2 \cdot 3 \cdots 2k},$$

sodass das Integral die Gestalt annimmt:

$$\sum_0^\infty {}_k \frac{(-1)^k x^{2k}}{1 \cdot 2 \cdot 3 \cdots 2k} \cdot \int_0^1 (1-z^2)^n \cdot z^{2k} dz,$$

so findet man sogleich bei Anwendung der Formel (14) die Beziehung:

$$\int_0^1 (1-z^2) \cdot \cos xz \, dz$$

$$= \sum_0^\infty {}_k \frac{(-1)^k x^{2k}}{1 \cdot 2 \cdot 3 \cdots 2k} \cdot \frac{2 \cdot 4 \cdot 6 \cdots 2n}{(2k+1)(2k+3) \cdots (2k+2n+1)},$$

d. h. nach (3) und (9) folgende Gleichung:

$$(15)\quad \psi(x)\sin x + \chi(x)\cos x = \frac{x^{2n+1}}{2\cdot 4\cdots 2n}\cdot\int_0^1 (1-z^2)^n \cos xz\,dz\,.$$

Hierin hat, wenn wir n als gerade Zahl voraussetzen, $\chi(x)$ die Bedeutung einer ungeraden Funktion vom Grade $n-1$, also die Gestalt

$$\chi(x) = x\cdot X(x^2)\,,$$

wenn unter $X(x^2)$ eine ganze und ganzzahlige Funktion des Grades $\frac{n}{2}-1$ von x^2 verstanden wird.

4. Aus der so nach Hermite gegebenen Gleichung (15) lassen sich mit Leichtigkeit die Sätze wieder finden, welche Lambert und Legendre bezüglich der Zahl π aus anderer Quelle hergeleitet haben: dass nämlich weder π selbst noch π^2 rational sein kann.

Denn setzt man

$$X(x^2) = Ax^{n-2} + A_1x^{n-4} + \cdots + A_{\frac{n}{2}-1}$$

und nimmt zunächst an, π sei rational, $\pi = \frac{b}{a}$, so ergiebt die Gleichung (15), wenn darin $x=\pi$ gesetzt wird,

$$-X(\pi^2) = \frac{\pi^{2n}}{2\cdot 4\cdot 6\cdots 2n}\cdot\int_0^1 (1-z^2)^n\cdot\cos\pi z\,dz$$

oder

$$(16)\qquad N = \frac{1}{a^2}\,\frac{\left(\frac{b^2}{2a}\right)^n}{1\cdot 2\cdot 3\cdots n}\cdot\int_0^1 (1-z^2)^n\cos\pi z\,dz,$$

wenn N eine ganze Zahl bedeutet. Wäre dagegen π^2 eine rationale Zahl, $\pi^2 = \frac{\beta}{\alpha}$, so fände man auf demselben Wege:

$$(17)\qquad N' = \frac{1}{\alpha}\cdot\frac{\left(\frac{\beta}{2\sqrt{\alpha}}\right)^n}{1\cdot 2\cdot 3\cdots n}\cdot\int_0^1 (1-z^2)^n\cos\pi z\,dz\,,$$

wo auch N' eine ganze Zahl bedeutet.

Das Integral ist < 1, da die Funktion unter dem Integralzeichen dauernd numerisch unter 1 bleibt; dass es nicht 0 ist, lässt sich einsehen, wenn man es zerlegt in

$$\int_0^{\frac{1}{2}} (1 - z^2)^n \cdot \cos \pi z \, dz + \int_{\frac{1}{2}}^1 (1 - z^2)^n \cdot \cos \pi z \, dz;$$

infolge des bekannten Mittelwerthsatzes aus der Theorie der bestimmten Integrale lässt sich das erste setzen gleich

$$(1 - \zeta^2)^n \cdot \int_0^{\frac{1}{2}} \cos \pi z \, dz = (1 - \zeta^2)^n \cdot \frac{1}{\pi},$$

das zweite gleich

$$(1 - \zeta'^2)^n \cdot \int_{\frac{1}{2}}^1 \cos \pi z \, dz = -(1 - \zeta'^2)^n \cdot \frac{1}{\pi},$$

wo ζ zwischen 0 und $\frac{1}{2}$, ζ' zwischen $\frac{1}{2}$ und 1 liegt; da hiernach $1 - \zeta^2 > 1 - \zeta'^2$ ist, kann das ganze Integral nicht verschwinden. Die Gleichungen (16) und (17), in welchen die (gerade) Zahl n beliebig gross gedacht werden kann, werden aber schliesslich unmöglich, wenn sie hinreichend gross gedacht wird. Denn bekanntlich nähert sich der Ausdruck $\frac{x^n}{1 \cdot 2 \cdot 3 \cdots n}$, wie gross der bestimmte Werth von x auch sei, mit unendlich wachsendem n der Null; für ein hinreichend grosses n werden demnach die Faktoren vor dem Integrale in den Formeln (16) und (17) beliebig klein sein, bei wachsendem n wird daher ein Augenblick eintreten, wo die rechten Seiten dieser Formeln, ohne zu verschwinden, unter die Einheit herabsinken, also keiner ganzen Zahl gleich sein können. Die Annahmen sind demnach unzulässig.

5. Im Vorigen haben wir nur die ersten Schritte auf dem von Hermite eröffneten Wege gethan und wollen nunmehr denselben weiter verfolgen.

Aus jeder der Grössen A_n bilden wir unbegrenzt viele andere A'_n, A''_n, A'''_n, $\cdots$, indem wir definiren:

$$A'_n = \int_0^x A_n\, dx, \quad A''_n = \int_0^x A'_n\, dx, \quad A'''_n = \int_0^x A''_n\, dx, \quad \cdots$$

Wählen wir hierbei zuerst für A_n den Ausdruck (3) in Gestalt einer Reihe:

$$A_n = \sum_{k=0}^{\infty} \frac{1}{(2k+1)(2k+3)\cdots(2k+2n+1)} \cdot \frac{(-1)^k x^{1+2k+2n}}{1\cdot 2\cdot 3\cdots 2k},$$

so findet sich ohne Schwierigkeit

$$A_n^i = \sum_{k=0}^{\infty} \frac{(2k+2)(2k+4)\cdots(2k+2n)\cdot(-1)^k x^{2k+2n+i+1}}{1\cdot 2\cdot 3\cdot 4\cdots(2k+2n+i+1)}$$

oder, wenn man setzt

$$(18) \qquad \mathfrak{A}_n^i = \sum_{k=0}^{\infty} \frac{(2k+2)(2k+4)\cdots(2k+2n)\cdot(-1)^k x^{2k}}{1\cdot 2\cdot 3\cdot 4\cdots(2k+2n+i+1)},$$

$$(19) \qquad A_n^i = x^{2n+i+1}\cdot \mathfrak{A}_n^i.$$

Aus der Formel (18) ergiebt sich, wenn darin $n+1$ statt n gesetzt wird,

$$\mathfrak{A}_{n+1}^i = \sum_{k=0}^{\infty} \frac{(2k+2)(2k+4)\cdots(2k+2n+2)\cdot(-1)^k x^{2k}}{1\cdot 2\cdot 3\cdots(2k+2n+i+1)(2k+2n+i+3)}.$$

Andererseits findet sich, wenn $\mathfrak{A}_n^i$ nach x differenzirt wird, wobei das $k=0$ entsprechende Glied verschwindet,

$$\frac{d\mathfrak{A}_n^i}{dx} = \sum_{k=1}^{\infty} \frac{2k(2k+2)\cdots(2k+2n)\cdot(-1)^k x^{2k-1}}{1\cdot 2\cdot 3\cdots(2k+2n+i+1)}$$

oder, wenn der Summationsbuchstabe k durch $k+1$ ersetzt wird,

$$-\frac{d\mathfrak{A}_n^i}{dx} = \sum_{k=0}^{\infty} \frac{(2k+2)(2k+4)\cdots(2k+2n+2)\cdot(-1)^k x^{2k+1}}{1\cdot 2\cdot 3\cdots(2k+2n+i+1)(2k+2n+i+3)}.$$

Durch Vergleichung mit $\mathfrak{A}_{n+1}^i$ erhält man sogleich die Beziehung

$$\mathfrak{A}_{n+1}^i = -\frac{1}{x}\cdot\frac{d\mathfrak{A}_n^i}{dx},$$

welche mit Rücksicht auf die Gleichung (19), die für jedes n besteht, leicht in die Form

$$A^i_{n+1} = (2n + i + 1)A^i_n - x \cdot \frac{dA^i_n}{dx}$$

gebracht werden kann. Nach den Definitionsgleichungen für die Grössen A^i_n ist aber $\frac{dA^i_n}{dx} = A^{i-1}_n$, also nimmt die vorstehende Gleichung folgende Gestalt an:

$$A^i_{n+1} = (2n + i + 1)A^i_n - x \cdot A^{i-1}_n . \tag{20}$$

Diese eigenthümliche Recursionsformel, welche gestattet, die Grössen A höherer Ordnung, d. h. mit grösseren Indices, aus denen geringerer Ordnung zu berechnen, verdient an sich volle Aufmerksamkeit. Beschränken wir uns z. B. auf den Index $i = 1$, so würde sie lauten:

$$A'_{n+1} = (2n + 2)A'_n - xA_n$$

und würde dazu dienen, vermittelst der Grössen $A, A_1, A_2, \cdots$ allmählich die Grössen $A'_1, A'_2, A'_3, \cdots$ aus A' zu berechnen.

Hier jedoch wollen wir den Gang dieser Rechnung nicht weiter verfolgen, sondern an die Definition der Grössen A^i_n wieder anknüpfen. Es war

$$A'_n = \int_0^x A_n \, dx ;$$

dies giebt, wenn für A_n jetzt der Ausdruck (9) gesetzt wird,

$$A'_n = \int_0^x (\psi(x) \sin x + \chi(x) \cos x) \, dx .$$

Aehnlich den Hilfsformeln (10) und (11) findet man

$$\begin{aligned} A'_n = \big(\Psi'(x) + X(x)\big) \sin x + \big(X'(x) - \Psi(x)\big) \cos x \\ + \Psi(0) - X'(0), \end{aligned} \tag{21}$$

wenn

$$\Psi(x) = \psi(x) - \psi''(x) + \psi''''(x) - \cdots$$
$$X(x) = \chi(x) - \chi''(x) + \chi''''(x) - \cdots$$

gesetzt wird. Wenn nun n gerade ist, so ist, wie gefunden worden, $\psi(x)$ und also auch $\Psi(x)$ eine gerade Funktion n^{ten}, $\chi(x)$ und daher auch $X(x)$ eine ungerade Funktion $(n-1)^{\text{ten}}$ Grades; daher wird der Faktor von $\sin x$ zur Rechten in (21) in diesem Falle eine ungerade Funktion $(n-1)^{\text{ten}}$ Grades, der Faktor von $\cos x$ eine gerade Funktion n^{ten} Grades sein. Ist im Gegentheil n ungerade, so findet sich in gleicher Weise der Faktor von $\sin x$ als eine ungerade Funktion n^{ten}, der von $\cos x$ als eine gerade Funktion $(n-1)^{\text{ten}}$ Grades. Endlich ist $\Psi(0) - X'(0)$ eine gewisse Konstante, welche C heisse. Setzt man

$$X'(x) - \Psi(x) = \psi_1(x), \quad \Psi'(x) + X(x) = \chi_1(x),$$

so verhalten sich $\psi_1(x)$, $\chi_1(x)$ ganz entsprechend den mit $\psi(x)$, $\chi(x)$ bezeichneten beiden Funktionen, und man hat

$$A_n' = \psi_1(x)\cos x + \chi_1(x)\sin x + C.$$

Eine neue Integration liefert

$$A_n'' = \int_0^x (\psi_1(x)\cos x + \chi_1(x)\sin x)\,dx + Cx$$

$$= (X_1'(x) + \Psi_1(x))\sin x + (\Psi_1'(x) - X_1(x))\cos x + Cx$$
$$+ X_1(0) - \Psi_1'(0).$$

Nach der angemerkten Natur der Funktionen $\psi_1(x)$, $\chi_1(x)$ aber ergiebt sich zunächst $X_1(0) = 0$, $\Psi_1'(0) = 0$, und wenn man dann

$$X_1'(x) + \Psi_1(x) = \psi_2(x), \quad \Psi_1'(x) - X_1(x) = \chi_2(x)$$

setzt, so verhalten sich die Funktionen $\psi_2(x)$, $\chi_2(x)$ wieder ganz genau so, wie die Funktionen $\psi(x)$, $\chi(x)$ resp., und die vorige Gleichung wird:

$$A_n'' = \psi_2(x)\sin x + \chi_2(x)\cos x + Cx.$$

In gleicher Weise findet man nunmehr leicht:

$$A_n''' = \psi_3(x)\cos x + \chi_3(x)\sin x + \frac{C}{2}x^2 + C'$$

$$A_n'''' = \psi_4(x)\sin x + \chi_4(x)\cos x + \frac{C}{6}x^3 + C'x$$

u. s. f. Man kann mit andern Worten folgendes allgemeine Ergebniss aussprechen: Jenachdem i gerade oder ungerade ist, findet man

$$A'_n = \psi_i(x) \sin x + \chi_i(x) \cos x + \varphi_i(x)$$

oder

$$A'_n = \psi_i(x) \cos x + \chi_i(x) \sin x + \varphi_i(x),$$

wobei $\psi_i(x)$ eine gerade Funktion n^{ten} oder $(n-1)^{\text{ten}}$, $\chi_i(x)$ eine ungerade Funktion $(n-1)^{\text{ten}}$ oder n^{ten} Grades bedeutet, jenachdem n gerade oder ungerade ist, während $\varphi_i(x)$ eine ganze Funktion von x ist, deren Grad gleichzeitig mit $i-1$ gerade oder ungerade ist.

6. Betrachtet man nun irgend zwei aufeinanderfolgende Glieder der Reihe A_n, A'_n, A''_n, A'''_n, $\cdots$, z. B. grösster Einfachheit wegen die beiden ersten Glieder:

$$\psi(x) \sin x + \chi(x) \cos x = A_n$$
$$\chi_1(x) \sin x + \psi_1(x) \cos x = A'_n - C,$$

so lassen sich die so gebildeten Gleichungen nach den Grössen $\sin x$, $\cos x$ auflösen und ergeben im betrachteten Falle:

$$\sin x \cdot R(x^2) = x \cdot T(x^2) + A_n \cdot \psi_1(x) - A'_n \cdot \chi(x)$$
$$\cos x \cdot R(x^2) = \qquad S(x^2) - A_n \cdot \chi_1(x) + A'_n \cdot \psi(x),$$

wenn $\psi(x)\psi_1(x) - \chi(x)\chi_1(x)$, was eine gerade Funktion von x vom Grade $2n$ ist, mit $R(x^2)$, die gerade Funktion $-C\cdot\psi(x)$ mit $S(x^2)$, die ungerade Funktion $C\cdot\chi(x)$ mit $x\cdot T(x^2)$ bezeichnet wird. Nach den für A_n, A'_n gegebenen Reihenausdrücken beginnen die nach steigenden Potenzen von x entwickelten, rechts noch ausser den ersten Gliedern stehenden Produkte offenbar erst mit x^{2n+1} bezw. x^{2n+2}. Denkt man sich also die Produkte $\sin x \cdot R(x^2)$, $\cos x \cdot R(x^2)$ gleichfalls nach den steigenden Potenzen von x entwickelt, und vernachlässigt alle Potenzen, welche die vom Grade $2n$ übersteigen, so müssen die Entwicklungen mit den ganzen Funktionen $x \cdot T(x^2)$, $S(x^2)$, deren Grade höchstens gleich n sind, bezw. übereinstimmen. Diesen Umstand wollen wir hinfort kurz in der Weise ausdrücken, dass wir sagen: $\sin x$, $\cos x$ seien bis auf Potenzen vom Grade $2n$ den rationalen Brüchen $\frac{x\,T(x^2)}{R(x^2)}$, $\frac{S(x^2)}{R(x^2)}$ bez. gleich, welche demnach als Näherungsbrüche mit demselben Nenner bezeichnet werden können.

Setzt man hierin, was wir uns einmal erlauben wollen wie Lambert, ohne die Berechtigung dazu näher zu erläutern, $\frac{x}{i}$ statt x, und benutzt die Formel

$$\cos\frac{x}{i} + i\cdot\sin\frac{x}{i} = e^x,$$

so entsteht aus den Gleichungen

$$\sin x = \frac{x\,T(x^2)}{R(x^2)}\cdots,\quad \cos x = \frac{S(x^2)}{R(x^2)}\cdots,$$

mit denen wir jenen Umstand ausdrücken, sogleich auch die folgende:

$$e^x = \frac{S(-x^2) + x\cdot T(-x^2)}{R(-x^2)}\cdots$$

oder kürzer

$$e^x = \frac{M(x)}{N(x)}\cdots$$

worin $M(x)$, $N(x)$ zwei ganze Funktionen von x, der Nenner insbesondere eine gerade Funktion von x vom Grade $2n$ ist; man findet also auch für die Exponentialfunktion e^x eine bis zu demselben Grade reichende Annäherung mittels einer rational gebrochenen Funktion.

7. Wenn wir von der besonderen Beschaffenheit der Funktionen $M(x)$, $N(x)$ absehen, können wir ganz im allgemeinen sagen: Die vorhergehenden Betrachtungen haben die Möglichkeit erwiesen, der Funktion e^x sich bis zu einem gewissen Grade durch einen rationalen Bruch anzunähern. Dass solche Annäherung sogar bis zu einem beliebigen Grade μ hin möglich ist, davon kann man sich leicht a priori überzeugen. Setzen wir nämlich die Gleichung an:

$$e^x = \frac{M(x)}{N(x)} + \cdots$$

mit Vernachlässigung von Potenzen vom Grade grösser als μ, d. h.

$$e^x\cdot N(x) - M(x) = \varepsilon_1 x^{\mu+1} + \varepsilon_2 x^{\mu+2} + \cdots, \tag{22}$$

und wählen die Grade der beiden Funktionen $M(x)$ und $N(x)$ gleich m, n resp. Wird für e^x seine Reihenentwicklung eingesetzt und die linke Seite der vorigen Gleichung nach steigenden Potenzen von x entwickelt gedacht, so muss man,

um der Gleichung zu genügen, die Coefficienten von x^0, x^1, x^2, $\cdots x^\mu$ gleich Null setzen, erhält also $\mu + 1$ offenbar homogene Gleichungen zwischen den Coefficienten der ganzen Funktionen $M(x)$ und $N(x)$, deren Anzahl gleich

$$(m + 1) + (n + 1) = m + n + 2$$

ist. Werden daher m, n so gewählt, dass ihre Summe $m + n = \mu$ ist, so dienen jene Bedingungsgleichungen genau zur Bestimmung der Verhältnisse der Coefficienten und, wenn etwa der Coefficient der höchsten Potenz in $N(x)$ angenommen, nämlich gleich 1 gewählt wird, zur Bestimmung der Coefficienten selbst, und die Möglichkeit der Annäherung ist dadurch erwiesen.

Aber man kann auch mit Hermite, ausgehend von einer elementaren Integralformel, für jeden gegebenen Grad μ Funktionen $\frac{M(x)}{N(x)}$ ohne Schwierigkeit finden, welche die Annäherung leisten.

Ist nämlich $F(z)$ eine Funktion von z, die wir für unsern Zweck sogleich als ganze Funktion vom Grade μ voraussetzen, und setzt man zur Abkürzung

$$\frac{F(z)}{x} + \frac{F'(z)}{x^2} + \cdots + \frac{F^{(\mu)}(z)}{x^{\mu+1}} = \mathfrak{F}(z), \tag{23}$$

so findet sich mittels partieller Integration die Formel:

$$\int e^{-zx} \cdot F(z)\, dz = -e^{-zx} \cdot \mathfrak{F}(z), \tag{24}$$

und folglich, wenn zwischen den Grenzen ζ, Z integrirt wird, die folgende:

$$\int_\zeta^Z e^{-zx} \cdot F(z)\, dz = e^{-\zeta x} \cdot \mathfrak{F}(\zeta) - e^{-Zx} \cdot \mathfrak{F}(Z). \tag{24a}$$

Werden nun ζ, Z als zwei verschiedene Wurzeln der Gleichung $F(z) = 0$, und zwar die erste als eine h-fache, die zweite als eine k-fache Wurzel vorausgesetzt, so verschwinden für $z = \zeta$ ausser der Funktion $F(z)$ auch ihre $h - 1$ ersten, für $z = Z$ ihre $k - 1$ ersten Ableitungen und es findet sich

$$\mathfrak{F}(\zeta) = \frac{F^{(h)}(\zeta)}{x^{h+1}} + \frac{F^{(h+1)}(\zeta)}{x^{h+2}} + \cdots + \frac{F^{(\mu)}(\zeta)}{x^{\mu+1}}$$

$$\mathfrak{F}(Z) = \frac{F^{(k)}(Z)}{x^{k+1}} + \frac{F^{(k+1)}(Z)}{x^{k+2}} + \cdots + \frac{F^{(\mu)}(Z)}{x^{\mu+1}},$$

d. h.

$$\mathfrak{F}(Z) = \frac{M(x)}{x^{\mu+1}}, \quad \mathfrak{F}(\zeta) = \frac{N(x)}{x^{\mu+1}}, \tag{25}$$

wenn $M(x)$ eine ganze Funktion vom Grade $m = \mu - k$, $N(x)$ eine ganze Funktion vom Grade $n = \mu - h$ bedeutet. Hiernach nimmt die Gleichung (24a) die Gestalt an:

$$e^{-\zeta x} \cdot N(x) - e^{-Zx} \cdot M(x) = x^{\mu+1} \cdot \int_{\zeta}^{Z} e^{-zx} F(z)\, dz \tag{26}$$

und liefert, wenn insbesondere $\zeta = 0$ angenommen wird, die folgende:

$$e^{Zx} \cdot N(x) - M(x) = x^{\mu+1} \cdot e^{Zx} \cdot \int_{0}^{Z} e^{-zx} F(z)\, dz. \tag{27}$$

Denkt man sich schliesslich hierin statt e^{Zx} und e^{-zx} zur Rechten der Gleichung ihre Reihenentwicklungen gesetzt und die ganze rechte Seite nach steigenden Potenzen von x entwickelt, so ist einleuchtend, dass die Entwicklung mit $x^{\mu+1}$ beginnt; demnach liefert vorstehende Gleichung eine, bis zum Grade μ reichende Annäherung an die Funktion e^{Zx} durch den Bruch $\frac{M(x)}{N(x)}$.

8. Z. B., wenn $F(z) = z^h (z-1)^k$ und $h + k = \mu$ gewählt wird, ergiebt sich aus (27) die besondere Formel:

$$e^x \cdot N(x) - M(x) = x^{\mu+1} \cdot e^x \cdot \int_0^1 e^{-zx} z^h (z-1)^k\, dz,$$

oder noch specieller, wenn $h = k$ also $\mu = 2h$ ist,

$$e^x \cdot N(x) - M(x) = x^{2h+1} \cdot e^x \int_0^1 e^{-zx} z^h (z-1)^h\, dz. \tag{28}$$

Die Funktionen $M(x)$ und $N(x)$ sind in diesem Falle leicht angebbar.

Aus $F(z) = z^h(z-1)^h$ folgt nämlich mittels des binomischen Satzes

$$F(z) = z^{2h} - \frac{h}{1} z^{2h-1} + \frac{h(h-1)}{1\cdot 2} z^{2h-2} - \cdots + (-1)^h \cdot z^h,$$

also durch i-malige Differenzirung,

$$\begin{aligned} F^{(i)}(z) = {} & 2h(2h-1)\cdots(2h-i+1)z^{2h-i} \\ & -\frac{h}{1}(2h-1)\cdots(2h-i)z^{2h-i-1} \\ & + \cdots\cdots\cdots\cdots \\ & + \frac{h(h-1)}{1\cdot 2}\cdot(h+2)\cdots(h-i+3)\cdot(-1)^{h+2}z^{h-i+2} \\ & + \frac{h}{1}\cdot(h+1)h\cdots(h-i+2)\cdot(-1)^{h+1}z^{h-i+1} \\ & + h\cdot(h-1)\cdots(h-i+1)\cdot(-1)^h z^{h-i}. \end{aligned}$$

Hieraus findet sich $F^{(i)}(0) = 0$, solange $i < h$ ist; ferner

$$F^{(h)}(0) = (-1)^h \cdot 1\cdot 2\cdot 3\cdots h$$

$$F^{(h+1)}(0) = (-1)^{h+1}\cdot\frac{h}{1}\cdot 1\cdot 2\cdot 3\cdots(h+1)$$

$$F^{(h+2)}(0) = (-1)^{h+2}\cdot\frac{h(h-1)}{1\cdot 2}\cdot 1\cdot 2\cdots(h+2)$$

u. s. f., allgemein für $r = 0, 1, 2, \cdots h$

$$F^{(h+r)}(0) = (-1)^{h+r}\cdot\frac{h(h-1)\cdots(h-r+1)}{1\cdot 2\cdots r}\cdot 1\cdot 2\cdot 3\cdots(h+r).$$

Nach den Ausdrücken für $\mathfrak{F}(\zeta)$, wo jetzt $\zeta = 0$ ist, ergiebt sich demnach

$$\begin{aligned} \frac{N(x)}{x^{2h+1}} = {} & \frac{(-1)^h\cdot 1\cdot 2\cdot 3\cdots h}{x^{h+1}} + (-1)^{h+1}\cdot\frac{h}{1}\cdot\frac{1\cdot 2\cdot 3\cdots(h+1)}{x^{h+2}} \\ & + (-1)^{h+2}\cdot\frac{h(h-1)}{1\cdot 2}\cdot\frac{1\cdot 2\cdot 3\cdots(h+2)}{x^{h+3}} + \cdots \\ & + (-1)^{2h}\cdot\frac{1\cdot 2\cdot 3\cdots 2h}{x^{2h+1}}, \end{aligned}$$

und folglich

$$\begin{aligned} N(x) = {} & (-1)^h\cdot 1\cdot 2\cdot 3\cdots h\cdot\Big[x^h - \frac{h}{1}\cdot(h+1)x^{h-1} + \\ & + \frac{h(h-1)}{1\cdot 2}(h+1)(h+2)x^{h-2} - \cdots + (-1)^h(h+1)(h+2)\cdots 2h\Big]. \end{aligned} \tag{29}$$

Andererseits ist $F(-z) = z^h(z+1)^h$ und, wenn $1+z$ statt z gesetzt wird, $F(1+z) = z^h(z+1)^h$, also

$$F(1+z) = F(-z),$$

woraus durch i-malige Differenzirung

$$F^{(i)}(1+z) = (-1)^i \cdot F^{(i)}(-z)$$

und für $z = 0$

$$F^{(i)}(1) = (-1)^i \cdot F^{(i)}(0)$$

gefunden wird. Nach den Ausdrücken für $\mathfrak{F}(Z)$, wo jetzt $Z = 1$ ist, wird demnach gewonnen:

$$\frac{M(x)}{x^{2h+1}} = \frac{1 \cdot 2 \cdot 3 \ldots h}{x^{h+1}} + \frac{h}{1} \cdot \frac{1 \cdot 2 \cdot 3 \ldots (h+1)}{x^{h+2}}$$
$$+ \frac{h(h-1)}{1 \cdot 2} \cdot \frac{1 \cdot 2 \cdot 3 \ldots (h+2)}{x^{h+3}} + \cdots + \frac{1 \cdot 2 \cdot 3 \ldots 2h}{x^{2h+1}},$$

und folglich

$$(30) \quad \begin{aligned} M(x) = 1 \cdot 2 \cdot 3 \cdots h \cdot \Big[x^h + \frac{h}{1} \cdot (h+1)\, x^{h-1} + \\ + \frac{h(h-1)}{1 \cdot 2} (h+1)(h+2)\, x^{h-2} + \cdots + (h+1)(h+2) \cdots 2h\Big]. \end{aligned}$$

Die so für $M(x)$ und $N(x)$ erhaltenen Ausdrücke (29) und (30) lehren, dass nicht nur die Coefficienten dieser beiden ganzen Funktionen, sondern auch noch diejenigen der Funktionen

$$\mathrm{M}(x) = \frac{M(x)}{1 \cdot 2 \cdot 3 \ldots h}, \quad \mathrm{N}(x) = \frac{N(x)}{1 \cdot 2 \cdot 3 \ldots h}$$

ganze Zahlen sind; und man findet zunächst aus (28) die Gleichung

$$(31) \quad e^x \cdot \mathrm{N}(x) - \mathrm{M}(x) = \frac{x^{2h+1}}{1 \cdot 2 \cdot 3 \ldots h} \cdot \int_0^1 e^{(1-z)x} \cdot z^h \cdot (z-1)^h \cdot dz.$$

Aus dieser aber lässt sich ohne Mühe der nach Lambert und Legendre aus anderer Quelle von uns bereits abgeleitete Satz, dass e^x irrational sei, sobald der Exponent x eine rationale Zahl ist, wiedergewinnen. Denn, wäre im Gegentheil, wenn x rational, $x = \frac{r}{s}$ ist, e^x eine rationale Zahl $\frac{a}{b}$, so nähme die vorige Gleichung, wie gross h auch gedacht wird, die Form an:

$$a \cdot \mathrm{N}(x) - b \cdot \mathrm{M}(x) = bx \cdot \frac{x^{2h}}{1 \cdot 2 \ldots h} \cdot \int_0^1 e^{(1-z)x} \cdot z^h (z-1)^h \, dz$$

oder auch

$$a \cdot N - b \cdot M = \frac{br}{s} \cdot \frac{\left(\frac{r^2}{s}\right)^h}{1 \,.\, 2 \,.\, 3 \ldots h} \cdot \text{Integral},$$

wo M, N ganze Zahlen bedeuten. Links steht demnach jetzt eine ganze Zahl. Eine solche Gleichung ist aber nicht für jedes noch so grosse h möglich; denn weil der Faktor

$$\frac{\left(\frac{r^2}{s}\right)^h}{1 \,.\, 2 \ldots h}$$

und damit auch die ganze rechte Seite mit wachsendem h gegen Null convergirt, wird der Ausdruck zur Rechten für hinreichend grosse Werthe von h, ohne Null zu werden, unter die Einheit herabsinken, dann also keiner ganzen Zahl mehr gleich sein können.

Siebente Vorlesung.

(Fortsetzung.)

1. Die zuletzt angestellten Betrachtungen lassen sich erheblich verallgemeinern. Sei nämlich jetzt

$$(1) \qquad F(z) = (z - z_0)^{m_0} \cdot (z - z_1)^{m_1} \cdots (z - z_n)^{m_n}$$

und setzen wir noch

$$(2) \qquad f(z) = (z - z_0)(z - z_1) \cdots (z - z_n)$$

und

$$(3) \qquad \mu = m_0 + m_1 + \cdots + m_n.$$

Aus dem allgemeinen Ausdrucke für $\mathfrak{F}(z)$ folgt dann sogleich

$$\mathfrak{F}(z_0) = \frac{N(x)}{x^{\mu+1}}, \quad \mathfrak{F}(z_1) = \frac{M_1(x)}{x^{\mu+1}}, \quad \cdots \quad \mathfrak{F}(z_n) = \frac{M_n(x)}{x^{\mu+1}},$$

wo unter $N(x)$ eine ganze Funktion von x vom Grade $\mu - m_0$, unter $M_1(x)$ eine solche vom Grade $\mu - m_1$, $\cdots$ unter $M_n(x)$ eine solche vom Grade $\mu - m_n$ zu verstehen ist. Aus der Formel (26) der vor. Vorlesung werden wir also für jeden Werth $i = 1, 2, 3, \cdots n$ die Gleichung erhalten:

$$(4) \quad e^{-z_0 x} \cdot N(x) - e^{-z_i x} \cdot M_i(x) = x^{\mu+1} \cdot \int_{z_0}^{z_i} e^{-zx} F(z)\, dz,$$

und diese giebt, wenn insbesondere $z_0 = 0$ angenommen wird, die folgenden Gleichungen:

$$e^{z_1 x} \cdot N(x) - M_1(x) = x^{\mu+1} \cdot \int_0^{z_1} e^{(z_1 - z)x} F(z)\, dz$$

$$e^{z_2 x} \cdot N(x) - M_2(x) = x^{\mu+1} \cdot \int_0^{z_2} e^{(z_2 - z)x} F(z)\, dz$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$e^{z_n x} \cdot N(x) - M_n(x) = x^{\mu+1} \cdot \int_0^{z_n} e^{(z_n - z)x} F(z)\, dz.$$

Da in den sämmtlichen rechten Seiten derselben, wenn sie nach steigenden Potenzen von x entwickelt gedacht werden, die niedrigste Potenz offenbar $x^{\mu+1}$ sein muss, so geben diese Gleichungen eine gleichzeitige Annäherung desselben Grades an die n Exponentialgrössen $e^{z_1 x}$, $e^{z_2 x}, \cdots e^{z_n x}$ vermittelst der n Näherungsbrüche

$$(5) \qquad \frac{M_1(x)}{N(x)}, \quad \frac{M_2(x)}{N(x)}, \quad \cdots \quad \frac{M_n(x)}{N(x)}$$

mit gleichem Nenner.

2. Mit der besonderen Wahl der Funktion $F(z)$, nämlich der Exponenten $m_0, m_1, \cdots m_n$ werden natürlich diese Näherungsbrüche sich ändern. Wir wollen z. B., indem wir alle Exponenten von gleichem Werthe m nehmen,

$$F(z) = f(z)^m$$

wählen; dieser Wahl entspricht dann also ein ganz bestimmtes System von Näherungsbrüchen (5). Jedoch wird dasselbe mit anderer Wahl des Exponenten m jedesmal ein anderes werden, ein anderes also, wenn für m allmählich erst $m + 1$, dann $m + 2, \cdots$ gesetzt wird. Es ist nun höchst beachtenswerth, dass zwischen den Zählern resp. Nennern der Näherungsbrüche dieser aufeinanderfolgenden Sy-

steme ein ähnlicher Zusammenhang besteht, wie dies bei den gewöhnlichen Kettenbrüchen der Fall ist: die Zähler nämlich und die Nenner der späteren Systeme lassen sich aus den entsprechenden Zählern resp. Nennern der früheren in gleichmässiger Weise berechnen. Dieser Umstand beruht aber darauf, dass — wenn wir hinfort mit Rücksicht auf unser eigentliches Vorhaben der Unbestimmten x den Werth 1 geben — in der Reihe der Integrale

$$\int_{z_0}^{z_i} e^{-z}\cdot f(z)^m\,dz,\quad \int_{z_0}^{z_i} e^{-z}\cdot f(z)^{m+1}\,dz,\quad \int_{z_0}^{z_i} e^{-z}\cdot f(z)^{m+2}\,dz$$

$$\cdots\cdots\cdots\cdots$$

die späteren in bestimmter Weise aus den früheren berechnet werden können. Die eigenthümliche Art der Berechnung, wie sie Hermite nachgewiesen hat, ist folgende:

Zunächst ergiebt sich durch partielle Integration die Richtigkeit der Formel

$$\int_{z_0}^{z_i} e^{-z}\cdot f(z)^m\,dz = m\cdot\int_{z_0}^{z_i} e^{-z}\cdot f(z)^{m-1}\cdot f'(z)\,dz,$$

welche, mit Hilfe der bekannten Differenzialbeziehung

$$\frac{f'(z)}{f(z)} = \frac{1}{z-z_0} + \frac{1}{z-z_1} + \cdots + \frac{1}{z-z_n}$$

die Gestalt annimmt:

$$\text{(6)}\qquad \begin{aligned} &\int_{z_0}^{z_i} e^{-z}\cdot f(z)^m\,dz \\ &= m\cdot\int_{z_0}^{z_i} e^{-z}\cdot\frac{f(z)^m}{z-z_0}\,dz + \cdots + m\cdot\int_{z_0}^{z_i} e^{-z}\cdot\frac{f(z)^m}{z-z_n}\,dz. \end{aligned}$$

Wir wollen, einer kurzen Bezeichnung halber, die einzelnen Integrale zur Rechten die Bestandtheile des auf der Linken stehenden Integrales nennen. Offenbar wird man nun aus diesem Integrale das folgende Integral

$$\int_{z_0}^{z_i} e^{-z}\cdot f(z)^{m+1}\,dz$$

berechnen können, wenn es möglich ist, seine Bestandtheile aus den Bestandtheilen des Integrales

$$\int_{z_0}^{z_i} e^{-z} \cdot f(z)^m dz$$

zu finden. Der Kern der ganzen Hermite'schen Betrachtung besteht nun in dem Nachweise, dass dieses der Fall ist, dass nämlich für jeden Werth ζ aus der Reihe $z_0, z_1, z_2, \ldots z_n$ eine Gleichung besteht von der Form:

$$(7)\quad \begin{aligned} &\int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^{m+1}}{z-\zeta} dz \\ &= k_0 \cdot \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z-z_0} dz + \cdots + k_n \cdot \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z-z_n} dz. \end{aligned}$$

3. Um diesen Nachweis zu führen, bemerken wir zuvörderst, dass die Summe

$$(8)\qquad \frac{k_0}{z-z_0} + \frac{k_1}{z-z_1} + \cdots + \frac{k_n}{z-z_n} = \frac{\psi(z)}{f(z)}$$

gesetzt werden kann, wenn unter $\psi(z)$ eine ganze Funktion vom Grade n verstanden wird; aber auch umgekehrt kann bei solcher Bedeutung von $\psi(z)$ der Bruch $\frac{\psi(z)}{f(z)}$ bekanntlich in Partialbrüche zerlegt und eine Gleichung von der Form (8) gebildet werden, in welcher dann die Zähler der Partialbrüche durch die Formeln

$$(9)\qquad k_0 = \frac{\psi(z_0)}{f'(z_0)}, \quad k_1 = \frac{\psi(z_1)}{f'(z_1)}, \quad \cdots \quad k_n = \frac{\psi(z_n)}{f'(z_n)}$$

gegeben sind. Hiernach ist die Gleichung (7) vollständig gleichbedeutend mit der folgenden:

$$(10)\qquad \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^{m+1}}{z-\zeta} dz = \int_{z_0}^{z_i} e^{-z} \cdot f(z)^m \cdot \frac{\psi(z)}{f(z)} dz,$$

wenn $\psi(z)$ als ganze Funktion vom n^{ten} Grade gedacht wird. Um aber jetzt zu zeigen, dass diese Gleichung für jedes $i = 1, 2, 3, \ldots n$ besteht, wenn diese Funktion $\psi(z)$ geeignet

gewählt wird, genügt es offenbar nachzuweisen, dass bei unbestimmter Integration die Beziehung

$$\int e^{-z} \cdot \frac{f(z)^{m+1}}{z-\zeta}\, dz = \int e^{-z} \cdot f(z)^m \frac{\psi(z)}{f(z)}\, dz - \Psi(z)$$

erfüllbar ist, indem man die Funktion $\Psi(z)$ so bestimmt, dass sie an den Grenzen der bestimmten Integrationen, d. h. für alle Werthe $z_0, z_1, z_2, \ldots z_n$ verschwindet; denn dann kommt man beim Uebergange zur Integration zwischen den Grenzen z_0, z_i auf die Gleichung (10) zurück. Jene Beziehung aber ist wieder mit der nachstehenden, welche durch Differenzirung daraus hervorgeht, völlig gleichbedeutend

$$(11) \qquad e^{-z} \cdot \frac{f(z)^{m+1}}{z-\zeta} = e^{-z} \cdot f(z)^m \cdot \frac{\psi(z)}{f(z)} - \Psi'(z);$$

und letztere lehrt, dass $e^z \cdot \Psi'(z)$ eine ganze, durch $f(z)^{m-1}$ theilbare Funktion von z sein müsste. Diese Bedingung und zugleich auch die andere, dass $\Psi(z)$ für alle Werthe $z_0, z_1, z_2, \ldots z_n$ verschwinde, wird aber erfüllt, wenn wir ansetzen:

$$(12) \qquad \Psi(z) = e^{-z} \cdot f(z)^m \cdot \varphi(z),$$

und unter $\varphi(z)$ eine ganze Funktion verstehen. Die Gleichung (11) nimmt dann leicht die Form an:

$$(13) \quad f(z) \cdot \frac{f(z)}{z-\zeta} = \psi(z) + [f(z) - m f'(z)]\, \varphi(z) - f(z)\, \varphi'(z),$$

in welcher wir versuchen wollen, ihr durch geeignete Wahl von $\varphi(z)$ und $\psi(z)$ zu genügen. Dass dies überhaupt und in völlig bestimmter Weise möglich ist, davon überzeugt man sich durch die Ueberlegung, dass auf der linken Seite eine ganze Funktion vom Grade $2n+1$ steht, rechts aber, wenn der Grad von $\varphi(z)$ gleich n gewählt wird, ebenfalls eine Funktion des $(2n+1)^{\text{ten}}$ Grades, und dass die Anzahl der Coefficienten von $\varphi(z)$ und $\psi(z)$ zusammen genommen genau $2n+2$ beträgt, sodass dieselben den $2n+2$ durch Identificirung beider Seiten entstehenden Bedingungsgleichungen zu genügen im stande und dadurch bestimmt sind. Zur wirklichen Berechnung von $\varphi(z)$ und $\psi(z)$ schreibe man die vorige Gleichung in der neuen Form:

$$(14) \qquad \frac{f(z)}{z-\zeta} = \frac{\psi(z)}{f(z)} + \left(1 - m \cdot \frac{f'(z)}{f(z)}\right) \varphi(z) - \varphi'(z).$$

Hier steht links eine ganze Funktion, rechts aber zunächst die echt gebrochene Funktion $\frac{\psi(z)}{f(z)}$; demnach ist offenbar die Funktion $\varphi(z)$ so zu wählen, dass die in dem Ausdrucke

$$\left(1 - m\frac{f'(z)}{f(z)}\right)\varphi(z) - \varphi'(z)$$

enthaltene ganze Funktion gleich $\frac{f(z)}{z-\zeta}$ wird. Nun ist

$$\frac{f'(z)}{f(z)} = \frac{1}{z-z_0} + \frac{1}{z-z_1} + \frac{1}{z-z_2} + \cdots + \frac{1}{z-z_n}$$

oder, wenn allgemein

(15) $$s_i = m(z_0^i + z_1^i + z_2^i + \cdots + z_n^i)$$

gesetzt wird,

$$m\cdot\frac{f'(z)}{f(z)} = \frac{s_0}{z} + \frac{s_1}{z^2} + \frac{s_2}{z^3} + \cdots;$$

setzt man daher noch

(16) $$\varphi(z) = \alpha_0 z^n + \alpha_1 z^{n-1} + \alpha_2 z^{n-2} + \cdots + \alpha_n,$$

also

$$\varphi'(z) = n\alpha_0 z^{n-1} + (n-1)\alpha_1 z^{n-2} + (n-2)\alpha_2 z^{n-3} + \cdots,$$

so muss schliesslich derjenige Bestandtheil des nach fallenden Potenzen von z entwickelten Ausdruckes

$$\left(1 - \frac{s_0}{z} - \frac{s_1}{z^2} - \frac{s_2}{z^3} - \cdots\right)\left(\alpha_0 z^n + \alpha_1 z^{n-1} + \alpha_2 z^{n-2} + \cdots\right)$$
$$- n\alpha_0 z^{n-1} - (n-1)\alpha_1 z^{n-2} - (n-2)\alpha_2 z^{n-3} - \cdots,$$

welcher die ganzen Potenzen von z enthält, gleich $\frac{f(z)}{z-\zeta}$ sein.

Da man aber, wenn

(17) $$f(z) = z^{n+1} + p_1 z^n + p_2 z^{n-1} + \cdots + p_{n+1}$$

und

(18) $$\zeta_i = \zeta^i + p_1\zeta^{i-1} + p_2\zeta^{i-2} + \cdots + p_i$$

gesetzt wird,

(18a) $$\frac{f(z)}{z-\zeta} = z^n + \zeta_1 z^{n-1} + \zeta_2 z^{n-2} + \cdots + \zeta_n$$

findet, so ergeben sich durch Vergleichung der entsprechenden Potenzen von z folgende Gleichungen:

$$(19)\quad \begin{cases} \alpha_0 = 1 \\ \alpha_1 - (s_0 + n)\alpha_0 = \zeta_1 \\ \alpha_2 - (s_0 + n - 1)\alpha_1 - s_1\alpha_0 = \zeta_2 \\ \alpha_3 - (s_0 + n - 2)\alpha_2 - s_1\alpha_1 - s_2\alpha_0 = \zeta_3 \\ \cdots\cdots\cdots\cdots \end{cases}$$

zur Bestimmung der Grössen α_i d. h. zur Bestimmung der Funktion $\varphi(z)$; und zwar findet man

$$(20)\quad \begin{cases} \alpha_0 = 1 \\ \alpha_1 = \zeta_1 + s_0 + n \\ \alpha_2 = \zeta_2 + (s_0 + n - 1)\zeta_1 + (s_0 + n)(s_0 + n - 1) + s_1 \\ \alpha_3 = \zeta_3 + (s_0 + n - 2)\zeta_2 + \big((s_0 + n - 1)(s_0 + n - 2) + s_1\big)\zeta_1 \\ \qquad + (s_0 + n)(s_0 + n - 1)(s_0 + n - 2) \\ \qquad + (2s_0 + 2n - 2)s_1 + s_2 \\ \cdots\cdots\cdots\cdots \end{cases}$$

Mit Beachtung der Definition der Zeichen p_i, ζ_i, wie sie aus (17) und (18) hervorgeht, findet man aus den vorstehenden Gleichungen allgemein α_i als eine ganze Funktion von ζ vom i^{ten} Grade, von deren Coefficienten der der höchsten Potenz gleich 1 ist, während die übrigen sich durch die ersten drei Rechnungsoperationen aus den Grössen p_i, s_i und ganzen Zahlen zusammensetzen, also ganze und ganzzahlige symmetrische Funktionen der Wurzeln $z_0, z_1, z_2, \cdots z_n$ der Gleichung $f(z) = 0$ sind. Demnach werden sie — nach den einfachsten Fundamentalsätzen aus der Theorie der Gleichungen — selbst ganze Zahlen sein, wenn die Coefficienten dieser Gleichung, insbesondere also, wenn die Wurzeln derselben ganze Zahlen sind. Wir wollen, um die Zusammensetzung der Grössen α_i anzudeuten, $\alpha_i = \varphi_i(\zeta)$ und demnach

$$(21)\qquad \varphi(z) = z^n + \varphi_1(\zeta)\cdot z^{n-1} + \cdots + \varphi_n(\zeta)$$

schreiben; desgleichen wollen wir, um die Abhängigkeit der Funktion $\varphi(z)$ von ζ zu bezeichnen, statt $\varphi(z)$ uns lieber des Zeichens $\varphi(z, \zeta)$ bedienen.

Ist durch diese Betrachtung die Funktion $\varphi(z)$ ermittelt, so findet sich jetzt sogleich aus (13)

$$\frac{\psi(z_0)}{f'(z_0)} = m \cdot \varphi(z_0, \zeta), \quad \cdots \quad \frac{\psi(z_n)}{f'(z_n)} = m \cdot \varphi(z_n, \zeta)$$

und daher nach den Formeln (8) und (9)

$$(22) \qquad \frac{\psi(z)}{f(z_0)} = \frac{m\,\varphi(z_0, \zeta)}{z - z_0} + \frac{m\,\varphi(z_1, \zeta)}{z - z_1} + \cdots + \frac{m\,\varphi(z_n, \zeta)}{z - z_n}.$$

Wir hatten voraufgeschickt, dass es wirklich zwei ganz bestimmte Funktionen $\varphi(z)$, $\psi(z)$ geben muss, welche die Gleichung (13) erfüllen; wir haben diese nunmehr in den Formeln (21), (22) ermittelt. Die hieraus entspringenden Funktionen $\psi(z)$, $\Psi(z)$ erfüllen demnach auch die Gleichung (11), daher $\psi(z)$ auch die Gleichung (10), sodass sich sogleich folgendes Gesammtergebniss herausstellt:

$$(23) \qquad \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^{m+1}}{z - \zeta}\, dz$$
$$= m \cdot \varphi(z_0, \zeta) \cdot \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z - z_0}\, dz + \cdots + m \cdot \varphi(z_n, \zeta) \cdot \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z - z_n}\, dz,$$

welches die Gleichung (7) ist, deren Bestand wir behauptet hatten.

4. Die Wurzel z_i ist eine beliebige unter den Grössen $z_1, z_2, \cdots z_n$, während dagegen ζ eine der Grössen $z_0, z_1, z_2, \cdots z_n$ bedeutet. Hält man zunächst z_i fest, lässt dagegen ζ seine Werthe durchlaufen, so entstehen aus der einen Gleichung (23) $n + 1$ Gleichungen. Um diese möglichst einfach zu schreiben, führen wir folgende Bezeichnungen ein:

$$(24) \qquad \begin{cases} \varepsilon_m = \dfrac{1}{1\,.\,2\,.\,3 \ldots m} \displaystyle\int_{z_0}^{z_i} e^{-z} \cdot f(z)^m\, dz \\[2ex] \varepsilon_m^h = \dfrac{1}{1\,.\,2\,.\,3 \ldots (m-1)} \displaystyle\int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z - z_h}\, dz. \end{cases}$$

Aus (6) folgt dann vor allem die Beziehung:

$$(25) \qquad \varepsilon_m = \varepsilon_m^0 + \varepsilon_m^1 + \varepsilon_m^2 + \cdots + \varepsilon_m^n,$$

und wenn in den genannten $n+1$ Gleichungen noch m in $m-1$ verwandelt wird — wobei wir die Bezeichnung der Coefficienten $\varphi(z_0, z_0)$ u. s. w. beibehalten, aber beachten müssen, dass sie natürlich bei der Verwandlung von m in $m-1$ zwar andere Werthe erhalten wie vorher, ohne jedoch ihren oben näher bezeichneten Charakter zu verlieren — so nehmen die $n+1$ Gleichungen folgende Gestalt an:

$$(26)\quad \begin{cases} \varepsilon_m^0 = \varphi(z_0, z_0)\varepsilon_{m-1}^0 + \varphi(z_1, z_0)\varepsilon_{m-1}^1 + \cdots + \varphi(z_n, z_0)\varepsilon_{m-1}^n \\ \varepsilon_m^1 = \varphi(z_0, z_1)\varepsilon_{m-1}^0 + \varphi(z_1, z_1)\varepsilon_{m-1}^1 + \cdots + \varphi(z_n, z_1)\varepsilon_{m-1}^n \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ \varepsilon_m^n = \varphi(z_0, z_n)\varepsilon_{m-1}^0 + \varphi(z_1, z_n)\varepsilon_{m-1}^1 + \cdots + \varphi(z_n, z_n)\varepsilon_{m-1}^n . \end{cases}$$

Indem nun hierin zunächst $m=2$, dann $m=3$ gewählt wird u. s. w., gewinnt man eine Reihe von Systemen linearer Gleichungen, welche offenbar gestatten, zuletzt die Grössen $\varepsilon_m^0, \varepsilon_m^1, \cdots \varepsilon_m^n$ linear auszudrücken durch die Grössen $\varepsilon_1^0, \varepsilon_1^1, \cdots \varepsilon_1^n$, sodass man setzen darf:

$$(27)\quad \begin{cases} \varepsilon_m^0 = A_0\varepsilon_1^0 + A_1\varepsilon_1^1 + \cdots + A_n\varepsilon_1^n \\ \varepsilon_m^1 = B_0\varepsilon_1^0 + B_1\varepsilon_1^1 + \cdots + B_n\varepsilon_1^n \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ \varepsilon_m^n = L_0\varepsilon_1^0 + L_1\varepsilon_1^1 + \cdots + L_n\varepsilon_1^n , \end{cases}$$

Gleichungen, über deren Determinante wir eine wichtige Bemerkung zu machen haben.

In der Determinante der Gleichungen (26), nämlich der Determinante

$$\begin{vmatrix} \varphi(z_0, z_0), & \varphi(z_1, z_0), & \cdots & \varphi(z_n, z_0) \\ \varphi(z_0, z_1), & \varphi(z_1, z_1), & \cdots & \varphi(z_n, z_1) \\ \cdot & \cdot & \cdot & \cdot \\ \varphi(z_0, z_n), & \varphi(z_1, z_n), & \cdots & \varphi(z_n, z_n) \end{vmatrix}$$

hat das allgemeine Glied die Gestalt

$$\varphi(z_i, z_k) = z_i^n + z_i^{n-1}\cdot\varphi_1(z_k) + \cdots + 1\cdot\varphi_n(z_k);$$

infolge dessen ist sie nach als bekannt vorauszusetzenden Sätzen der Determinantentheorie das Produkt nachstehender zwei Determinanten:

$$\varDelta = \begin{vmatrix} z_0^n, & z_1^n, & \dots & z_n^n \\ z_0^{n-1}, & z_1^{n-1}, & \dots & z_n^{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ z_0, & z_1, & \dots & z_n \\ 1, & 1, & \dots & 1 \end{vmatrix},$$

welche bekanntlich das Produkt der Wurzeldifferenzen $z_i - z_k$ vorstellt, und

$$Z = \begin{vmatrix} 1, & 1, & \dots & 1 \\ \varphi_1(z_0), & \varphi_1(z_1), & \dots & \varphi_1(z_n) \\ \cdot & \cdot & \cdot & \cdot \\ \varphi_i(z_0), & \varphi_i(z_1), & \dots & \varphi_i(z_n) \\ \cdot & \cdot & \cdot & \cdot \\ \varphi_n(z_0), & \varphi_n(z_1), & \dots & \varphi_n(z_n) \end{vmatrix}.$$

In der letztern aber ist — nach den über $\alpha_i = \varphi_i(\zeta)$ gemachten Bemerkungen —

$$\varphi_i(z_0) = z_0^i + c_1 z_0^{i-1} + \cdots + c_{i-1} z_0 + c_i$$
$$\cdots\cdots\cdots\cdots$$
$$\varphi_i(z_n) = z_n^i + c_1 z_n^{i-1} + \cdots + c_{i-1} z_n + c_i;$$

ihre $(i+1)^{\text{te}}$ Horizontalreihe entsteht also aus der (von unten gerechnet) $(i+1)^{\text{ten}}$ Horizontalreihe der Determinante $\varDelta$, indem dazu die unteren Reihen derselben mit $c_1, \dots c_{i-1}, c_i$ bezüglich multiplicirt hinzugefügt werden, ein Verfahren, welches bekanntlich den Werth der Determinante $\varDelta$ nicht ändert. Und somit ergiebt sich $Z = \varDelta$, d. h. die Determinante der Gleichungen (26) hat den Werth $\varDelta^2$, welchen Werth man für m auch vorausgesetzt hat. Da nun die Determinante der Gleichungen (27), den Gesetzen der Zusammensetzung linearer Gleichungssysteme gemäss, das Produkt aus den Determinanten der $m-1$ aufeinanderfolgenden Systeme linearer Gleichungen ist, aus deren Zusammensetzung jene entstanden, so findet sich sogleich für die Determinante der Gleichungen (27) der Werth $\varDelta^{2(m-1)}$. Die Wurzeln $z_0, z_1, z_2, \dots z_n$ der Gleichung $f(z) = 0$ werden aber als von einander verschieden vorausgesetzt; daher ist $\varDelta$ und somit auch jene Determinante verschieden von Null.

5. Um zur Einsetzung in die Gleichungen (27) die Werthe der Grössen ε_1^h zu ermitteln, gehen wir aus von der Betrachtung des Integrales

$$\int e^{-z} \cdot \frac{f(z)}{z-\zeta} \cdot dz,$$

in welchem ζ irgend eine der Wurzeln $z_0, z_1, z_2, \ldots z_n$ der Gleichung $f(z) = 0$ bedeuten soll. Man findet es zunächst nach (18) und (18a) gleich

$$\int e^{-z} \cdot \{z^n + (\zeta + p_1) z^{n-1} + (\zeta^2 + p_1 \zeta + p_2) z^{n-2} + \cdots$$
$$+ \zeta^n + p_1 \zeta^{n-1} + p_2 \zeta^{n-2} + \cdots + p_n\} dz,$$

und da nach der Hermite'schen Grundformel — (24) vor. Vorlesung — sogleich gefunden wird:

$$\int e^{-z} \cdot z^m dz = -e^{-z}\left(z^m + m z^{m-1} + m(m-1) z^{m-2} + \cdots\right),$$

so kann man setzen:

$$\int e^{-z} \cdot \frac{f(z)}{z-\zeta} dz = -e^{-z} \cdot \Phi(z, \zeta), \tag{28}$$

wobei die Funktion $\Phi(z, \zeta)$ statt der Summe

$$z^n + n z^{n-1} + n(n-1) z^{n-2} + \cdots$$
$$+ (\zeta + p_1)\left(z^{n-1} + (n-1) z^{n-2} + \cdots\right)$$
$$+ (\zeta^2 + p_1 \zeta + p_2)(z^{n-2} + \cdots)$$
$$+ \cdots + \zeta^n + p_1 \zeta^{n-1} + \cdots + p_n$$

steht, also gleich

$$z^n + (\zeta + p_1 + n) z^{n-1}$$
$$+ \left(\zeta^2 + (p_1 + n - 1)\zeta + p_2 + (n-1) p_1 + n(n-1)\right) z^{n-2}$$
$$+ \cdots$$

ist. Wenn man folglich schreibt

$$\Phi(z, \zeta) = z^n + \varphi^1(\zeta) \cdot z^{n-1} + \varphi^2(\zeta) \cdot z^{n-2} + \cdots + \varphi^n(\zeta),$$

so wird $\varphi^i(\zeta)$, wie früher die Funktion $\varphi_i(\zeta)$, eine ganze Funktion von ζ vom i^{ten} Grade, von deren Coefficienten der höchste gleich 1, die übrigen ganze und ganzzahlige symmetrische Funktionen der Wurzeln $z_0, z_1, z_2, \ldots z_n$, also

ganze Zahlen sind, so oft die letzteren es sind. In diesem Falle werden demnach auch die sämmtlichen Werthe $\Phi(z_i, z_k)$ ganze Zahlen sein, und aus der Zusammensetzung von $\Phi(z, \zeta)$, welche derjenigen von $\varphi(z, \zeta)$ gänzlich analog ist, schliesst man, gerade wie es für die Determinante der Grössen $\varphi(z_i, z_k)$ geschehen ist, dass auch die Determinante der Grössen $\Phi(z_i, z_k)$ gleich Δ^2 also von Null verschieden ist.

Nunmehr ergiebt sich mit Rücksicht auf die Definitionsgleichungen (24) nach der Formel (28) der Werth

$$\varepsilon_1^h = e^{-z_0} \cdot \Phi(z_0, z_h) - e^{-z_i} \cdot \Phi(z_i, z_h). \tag{29}$$

Wenn wir also, um die Abhängigkeit der Grössen ε_m^h auch von z_i anzudeuten, jetzt lieber $\varepsilon_{i,m}^h$ statt ε_m^h setzen, so werden die Gleichungen (27) folgende Gestalt annehmen:

$$(30)\quad \begin{cases} \varepsilon_{i,m}^0 = e^{-z_0} \cdot \alpha_0 - e^{-z_i} \cdot \alpha_i \\ \varepsilon_{i,m}^1 = e^{-z_0} \cdot \beta_0 - e^{-z_i} \cdot \beta_i \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ \varepsilon_{i,m}^n = e^{-z_0} \cdot \lambda_0 - e^{-z_i} \cdot \lambda_i, \end{cases}$$

in welcher gesetzt ist

$$(31)\quad \begin{cases} \alpha_i = A_0 \cdot \Phi(z_i, z_0) + A_1 \cdot \Phi(z_i, z_1) + \cdots + A_n \Phi(z_i, z_n) \\ \beta_i = B_0 \cdot \Phi(z_i, z_0) + B_1 \cdot \Phi(z_i, z_1) + \cdots + B_n \Phi(z_i, z_n) \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ \lambda_i = L_0 \cdot \Phi(z_i, z_0) + L_1 \cdot \Phi(z_i, z_1) + \cdots + L_n \Phi(z_i, z_n). \end{cases}$$

So oft die Wurzeln $z_0, z_1, z_2, \ldots z_n$ als ganze Zahlen vorausgesetzt werden, werden auch diese Grössen $\alpha_i, \beta_i, \ldots \lambda_i$ sämmtlich ganzzahlig sein; denn dann werden nicht nur, wie bemerkt, die sämmtlichen Grössen $\Phi(z_i, z_k)$, sondern aus gleichen Gründen auch die sämmtlichen Grössen $\varphi(z_i, z_k)$ und demnach auch die aus Ausdrücken dieser Art nur durch Additionen, Subtraktionen und Multiplikationen zusammengesetzten Coefficienten $A, B, \ldots L$ ganze Zahlen sein.

6. So haben wir die Grundlage gewonnen, auf welcher nun der Hermite'sche Satz, dass die Zahl e transcendent sei, sehr einfach erwiesen werden kann. Denn, wäre im Gegentheil e eine algebraische Zahl, d. h. Wurzel einer algebraischen

Gleichung mit rationalen Coefficienten, so müsste eine Beziehung stattfinden von folgender Form:

$$e^{z_0}\cdot N_0 + e^{z_1}\cdot N_1 + \cdots + e^{z_n}\cdot N_n = 0\,, \tag{32}$$

in welcher die N_i ganze, von Null verschiedene Zahlen, die Exponenten $z_0, z_1, z_2, \ldots z_n$ aber positive ganze Zahlen (Null einschliesslich) wären. Nun ergiebt sich aber, indem diese ganzen Zahlen jetzt zu Wurzeln der Gleichung $f(z) = 0$ gewählt werden, aus der ersten der Gleichungen (30), wenn i die Werthe 1, 2, 3, ... n erhält,

$$\begin{aligned}
\overset{0}{\varepsilon}_{1,m} &= e^{-z_0}\cdot\alpha_0 - e^{-z_1}\cdot\alpha_1\\
\overset{0}{\varepsilon}_{2,m} &= e^{-z_0}\cdot\alpha_0 - e^{-z_2}\cdot\alpha_2\\
&\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\\
\overset{0}{\varepsilon}_{n,m} &= e^{-z_0}\cdot\alpha_0 - e^{-z_n}\cdot\alpha_n\,,
\end{aligned}$$

und, wenn diese Gleichungen der Reihe nach mit $e^{z_1}N_1$, $e^{z_2}N_2, \ldots e^{z_n}N_n$ multiplicirt und dann addirt werden, die nachstehende Gleichung:

$$\begin{aligned}
&e^{z_1}\cdot\overset{0}{\varepsilon}_{1,m}\cdot N_1 + e^{z_2}\cdot\overset{0}{\varepsilon}_{2,m}\cdot N_2 + \cdots + e^{z_n}\cdot\overset{0}{\varepsilon}_{n,m}\cdot N_n\\
&= e^{-z_0}\alpha_0\,(e^{z_1}N_1 + e^{z_2}N_2 + \cdots + e^{z_n}N_n)\\
&- (\alpha_1 N_1 + \alpha_2 N_2 + \cdots + \alpha_n N_n)\,.
\end{aligned}$$

Diese nimmt aber unter der gemachten Voraussetzung, dass die Gleichung (32) besteht, die Form an:

$$\begin{aligned}
&\alpha_0 N_0 + \alpha_1 N_1 + \alpha_2 N_2 + \cdots + \alpha_n N_n\\
&= -\,(e^{z_1}\overset{0}{\varepsilon}_{1,m}N_1 + e^{z_2}\overset{0}{\varepsilon}_{2,m}N_2 + \cdots + e^{z_n}\overset{0}{\varepsilon}_{n,m}N_n)\,.
\end{aligned} \tag{33}$$

Hier steht links eine ganze Zahl. Da man andererseits, dem bekannten Mittelwerthsatze der Theorie der bestimmten Integrale gemäss,

$$\overset{0}{\varepsilon}_{i,m} = \frac{1}{1\,.\,2\,.\,3\,\ldots\,(m-1)}\cdot\int_{z_0}^{z_i} e^{-z}\cdot\frac{f(z)^m}{z - z_0}\,dz$$

gleich

$$\begin{aligned}
&\frac{1}{1\,.\,2\,.\,3\,\ldots\,(m-1)}\cdot\frac{f(\xi)^m}{\xi - z_0}\cdot\int_{z_0}^{z_i} e^{-z}\,dz\\
&= \frac{f(\xi)}{\xi - z_0}\cdot\frac{f(\xi)^{m-1}}{1\,.\,2\,.\,3\,\ldots\,(m-1)}\cdot(e^{-z_0} - e^{-z_i})
\end{aligned}$$

setzen darf, wo unter ξ ein gewisser Werth zwischen den Grenzen z_0, z_i zu verstehen ist, und da folglich mit unendlich wachsendem m der Werth von $\varepsilon_{i,m}^0$ zugleich mit dem zweiten Faktor des letzten Ausdruckes unendlich abnimmt, welchen Werth i auch hat, so wird die rechte Seite der Gleichung (33) mit wachsendem m unter jeden Grad von Kleinheit herabsinken, von einem gewissen Augenblicke an folglich unter der Einheit liegen, also die Gleichung (33) nicht, wie sie doch erhalten ist, für jeden Werth von m möglich sein, wenn nicht die ganze Zahl links gleich Null ist. So gelangt man zu der ersten Gleichung des nachfolgenden Systems:

$$\alpha_0 N_0 + \alpha_1 N_1 + \alpha_2 N_2 + \cdots + \alpha_n N_n = 0$$
$$\beta_0 N_0 + \beta_1 N_1 + \beta_2 N_2 + \cdots + \beta_n N_n = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\lambda_0 N_0 + \lambda_1 N_1 + \lambda_2 N_2 + \cdots + \lambda_n N_n = 0,$$

deren übrige auf ähnlichem Wege erschlossen werden und welche sämmtlich von einem gewissen Werthe von m an dauernd bestehen müssen. Das ist nicht anders möglich, als wenn ihre aus den Grössen α_i, β_i, ... λ_i gebildete Determinante verschwindet, und dies wieder kann nicht geschehen, da jene Determinante, wie die Gleichungen (31) sogleich darthun, das Produkt zweier Determinanten ist, deren eine gleich $\Delta^{2(m-1)}$, deren andere gleich Δ^2 gefunden wurde, das Produkt also zweier Faktoren, welche beide, wie Δ selbst, von Null verschieden sind.

Hieraus folgt die Unmöglichkeit jeder Beziehung von der Form (32) und daher auch die Transcendenz der Zahl e.

7. Wir setzen zum Beschluss dieser Betrachtungen beispielsweise $n = 1$ und $f(z) = z(z-x)$ voraus. Dann hat man nach (24)

$$\varepsilon_m = \frac{1}{1 \cdot 2 \cdot 3 \ldots m} \cdot \int_0^x e^{-z} \cdot z^m (z-x)^m \, dz$$

$$\varepsilon_m^0 = \frac{1}{1 \cdot 2 \cdot 3 \ldots (m-1)} \cdot \int_0^x e^{-z} \cdot z^{m-1} (z-x)^m \, dz$$

$$\overset{1}{\varepsilon}_m = \frac{1}{1 \cdot 2 \cdot 3 \ldots (m-1)} \cdot \int_0^x e^{-z} \cdot z^m (z-x)^{m-1} dz;$$

ferner ist

$$\varphi(z, \zeta) = z + (\zeta_1 + s_0 + 1)$$
$$f(z) = z^2 - xz,$$

also

$$p_1 = -x, \quad \zeta_1 = \zeta + p_1 = \zeta - x, \quad s_0 = 2m$$

und daher

$$\varphi(z, \zeta) = z + (\zeta + 2m + 1 - x).$$

Demnach liefern die Gleichungen (26), wenn m um eine Einheit vergrössert wird,

$$\overset{0}{\varepsilon}_{m+1} = (2m + 1 - x)\overset{0}{\varepsilon}_m + (2m+1)\overset{1}{\varepsilon}_m$$
$$\overset{1}{\varepsilon}_{m+1} = (2m+1)\overset{0}{\varepsilon}_m + (2m + 1 + x)\overset{1}{\varepsilon}_m,$$

woraus durch Subtraktion und mit Rücksicht auf die Gleichung $\varepsilon_m = \overset{0}{\varepsilon}_m + \overset{1}{\varepsilon}_m$ die folgende:

(34) $$\overset{1}{\varepsilon}_{m+1} - \overset{0}{\varepsilon}_{m+1} = x \cdot \varepsilon_m,$$

durch Addition und mit Rücksicht auf die Gleichung $\overset{0}{\varepsilon}_{m+1} + \overset{1}{\varepsilon}_{m+1} = \varepsilon_{m+1}$ die andere:

(35) $$\varepsilon_{m+1} = (4m+2)\varepsilon_m + x(\overset{1}{\varepsilon}_m - \overset{0}{\varepsilon}_m)$$

hervorgeht. Da aus (34) aber

$$\overset{1}{\varepsilon}_{m+1} = \frac{\varepsilon_{m+1} + x \cdot \varepsilon_m}{2}$$

$$\overset{0}{\varepsilon}_{m+1} = \frac{\varepsilon_{m+1} - x \cdot \varepsilon_m}{2}$$

oder, indem m in $m - 1$ verwandelt wird, für $m > 1$

$$\overset{1}{\varepsilon}_m = \frac{\varepsilon_m + x\varepsilon_{m-1}}{2}$$

$$\overset{0}{\varepsilon}_m = \frac{\varepsilon_m - x\varepsilon_{m-1}}{2}$$

gefunden wird, so nimmt die zuletzt erhaltene Gleichung für $m > 1$ die Gestalt an:

(36) $$\varepsilon_{m+1} = (4m+2)\varepsilon_m + x^2 \cdot \varepsilon_{m-1}.$$

Dieselbe gilt jedoch auch für $m = 1$: denn man findet ohne Mühe die Formeln:

$$\varepsilon_0 = 1 - e^{-x}, \quad \varepsilon_1 = 2 - x - e^{-x}(2 + x)$$
$$\varepsilon_2 = 12 - 6x + x^2 - e^{-x}(12 + 6x + x^2)$$

und vermittelst derselben in der That

$$\varepsilon_2 = 6 \cdot \varepsilon_1 + x^2 \cdot \varepsilon_0 .$$

Aus der so gewonnenen Reduktionsformel, welche der Formel (8) der vorigen Vorlesung völlig analog ist, geht nun für $\frac{\varepsilon_1}{\varepsilon_0}$ ein Kettenbruch, und da

$$\frac{\varepsilon_1}{\varepsilon_0} = 2 - \frac{e^x + 1}{e^x - 1} \cdot x$$

ist, folgender Kettenbruch hervor:

$$\frac{e^x - 1}{e^x + 1} = \cfrac{x}{2 + \cfrac{x^2}{6 + \cfrac{x^2}{10 + \cfrac{x^2}{14 + \cdots}}}},$$

welcher sich sogleich in den früher nach Lambert für

$$\frac{e^x - e^{-x}}{e^x + e^{-x}}$$

angegebenen verwandelt, wenn $2x$ statt x eingeführt und die Gleichheit

$$\frac{e^{2x} - 1}{e^{2x} + 1} = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

beachtet wird.

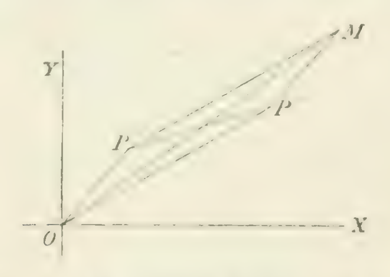
Achte Vorlesung.

Die Ludolph'sche Zahl π.

1. Wir wenden uns nunmehr zur Betrachtung der Zahl π und beginnen mit einer allgemeinen Vorbemerkung. Bei den Hermite'schen Untersuchungen verstanden wir unter z_0, z_1, z_2, . . . z_n stets reelle, zuletzt sogar ganze reelle Zahlen; im

Folgenden wird z_0 stets gleich Null, $z_1, z_2, \ldots z_n$ werden jedoch als die Wurzeln einer beliebigen Gleichung n^{ten} Grades mit ganzzahligen Coefficienten vorausgesetzt werden, und demnach auch imaginäre oder allgemeiner complexe Werthe bedeuten können. Die Grössen, welche unter (24) vor. Vorlesung mit ε_n, ε_n' bezeichnet worden sind, werden dann aber bestimmte Integrale, deren Grenzen imaginär sind, und bei denen also die Veränderliche z eine complexe Werthreihe, einen sogenannten complexen Integrationsweg durchläuft. Auf die Theorie der complexen Funktionen und ihrer Integrale hier näher einzugehen, können wir uns nicht gestatten, jedoch mögen einige wenige Punkte, auf die es hier ankommt, kurz erwähnt oder in Erinnerung gerufen werden.

Eine complexe Grösse $x + yi$ lässt sich durch denjenigen Punkt einer Ebene geometrisch darstellen, welchem die rechtwinkligen Coordinaten x, y entsprechen, oder, was dasselbe ist, wenn $x + yi$ in der „Normalform“ $r(\cos\varphi + i\sin\varphi)$ geschrieben wird, durch den Punkt P mit den Polarcoordinaten r, φ oder auch durch den nach Grösse und Richtung gedachten Radiusvektor OP, welcher vom Coordinatenanfangspunkte O nach P hinführt. Die Grösse dieses Radiusvektors, $r = \sqrt{x^2 + y^2}$, ist der sogenannte Modulus oder absolute Betrag der complexen Grösse $x + yi$.



Entsprechen so die Punkte P, P' den zwei complexen Grössen $x + yi$, $x' + y'i$, so wird die Differenz zwischen letzteren, $(x' + y'i) - (x + yi)$, durch die, nach Grösse und Richtung gedachte Strecke PP' geometrisch dargestellt; die Summe beider dagegen durch die andere Diagonale OM des über OP und OP' gezeichneten Parallelogramms. Aus diesem

letzteren Umstande folgt nach bekanntem Dreieckssatze leicht folgender

Satz: Der Modulus einer Summe zweier complexer Grössen ist niemals grösser als die Summe der Moduln der complexen Grössen selbst; ein Satz, der auf beliebig viel Summanden sofort erweitert werden kann.

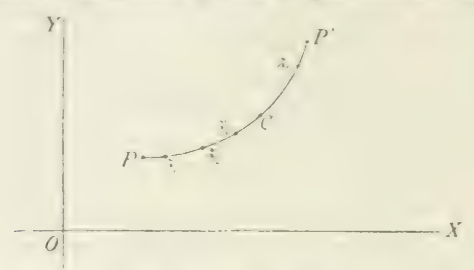
Da jeder complexen Grösse ein Punkt der Ebene entspricht, wird einer veränderlichen complexen Grösse ein beweglicher Punkt entsprechen, und einer stetigen Reihe complexer Werthe eine zusammenhängende Curve, welche der entsprechende Punkt beschreibt, und welche der Weg der complexen Veränderlichen genannt wird; und umgekehrt entspricht jedem beliebigen Wege zwischen zwei Punkten P, P' eine stetige Werthreihe der complexen Veränderlichen. Da es unendlich viel verschiedene solche Wege giebt, ist's auch einer complexen Veränderlichen möglich, auf unendlich mannigfaltige Weise stetig von einem bestimmten Werthe zu einem zweiten überzugehen.

Eine complexe Grösse $w = u + vi$, welche für jeden Werth einer complexen Veränderlichen $z = x + yi$ einen gleichfalls bestimmten Werth hat und sich also im allgemeinen gleichzeitig mit z verändert, heisst — nach Riemann — eine Funktion von z, $w = f(z)$, wenn sie der partiellen Differenzialgleichung $\frac{\partial w}{\partial y} = i \frac{\partial w}{\partial x}$ genügt; sie heisst stetig längs eines bestimmten Weges der Veränderlichen z, wenn der sie darstellende Punkt, während z jenen Weg beschreibt, gleichfalls eine stetig zusammenhangende Curve, d. i. einen Weg durchläuft.

Man denke sich nun zwei complexe Werthe ζ, ζ' und zwischen ihnen einen beliebig gegebenen Weg, dargestellt bez. durch die Punkte P, P' und die Curve PCP'. Zwischen den Endpunkten denke man beliebig viel, beliebig nahe Zwischenpunkte z_1, z_2, ... z_n eingeschaltet und bezeichne die ihnen entsprechenden complexen Werthe gleichfalls durch $z_1, z_2, \ldots z_n$. Mit ζ_0, ζ_1, ζ_2, ... ζ_n bezeichne man Punkte innerhalb der einzelnen Abschnitte Pz_1, z_1z_2, z_2z_3, ... z_nP' der Curve, bez. die ihnen entsprechenden complexen Werthe, und mit $f(z)$ irgend eine Funktion von z. Die folgende Summe:

$$(1)\quad S = f(\zeta_0)(z_1 - \zeta) + f(\zeta_1)(z_2 - z_1) + f(\zeta_2)(z_3 - z_2) + \cdots + f(\zeta_n)\cdot(\zeta' - z_n)$$

hängt dann zwar offenbar ab sowohl von der Anzahl, als auch von der Lage der einzelnen Zwischenwerthe auf der Curve, und folglich auch von dem bestimmten Wege der Veränderlichen z, welcher zwischen ζ und ζ' gewählt worden ist; aber



es lässt sich zeigen, dass, wenn die Menge der Zwischenwerthe durch stets fortgesetzte Einschaltung unendlich wächst und die Zwischenwerthe zugleich einander unendlich nahe rücken, jene Summe im allgemeinen für jeden bestimmten Weg gegen einen gleichfalls ganz bestimmten Grenzwerth convergirt, welcher das, diesem bestimmten Integrationswege entsprechende Integral von $f(z)$, in Zeichen:

$$\int_{\zeta}^{\zeta'} f(z)\,dz,$$

genannt wird; und ferner, dass die, den verschiedensten, zwischen ζ und ζ' möglichen Integrationswegen entsprechenden Integrale gleichwerthig, das Integral mit andern Worten unabhängig ist vom Integrationswege, vorausgesetzt, dass jene Wege gewisse Punkte der Ebene, welche kritische Punkte der Funktion $f(z)$ heissen, nicht mitsammen umschliessen.

2. Für die oben erwähnten, mit ε_m, ε_m^h bezeichneten Integrale wäre der einzige, dem Faktor e^{-z} der zu integrirenden Funktion entspringende kritische Punkt der Unendlichkeitspunkt der Ebene, $z = \infty$. Wir wollen ihn ausschliessen, d. h. die Integrationswege, sonst zwar beliebig, doch so gewählt voraussetzen, dass sie nicht durch $z = \infty$ hindurchführen;

dann haben ε_m, ε_m^h ganz bestimmte, vom Integrationswege unabhängige endliche Werthe, die freilich complex sein werden. Trotz dieser wesentlichen Aenderung des arithmetischen Verhaltens der Grössen ε_m, ε_m^h werden aber gleichwohl die Beziehungen (25) und (26), sowie die daraus abgeleiteten Gleichungen (27), (30) und (31) vor. Vorlesung bestehen bleiben; denn sie ergeben sich aus den Formeln, welche in No. 1—3 jener Vorlesung enthalten sind, und diese sprechen lediglich identische Umformungen aus und müssen deshalb sowohl für reelle, wie für complexe Werthe der Grössen z und $z_1, z_2, \ldots z_n$ in Geltung bleiben.

Da ferner, wie in No. 3 vor. Vorlesung bemerkt worden ist, die Funktion $\varphi_i(\zeta)$ eine ganze Funktion von ζ mit ganzzahligen Coefficienten ist, wenn, wie hier vorausgesetzt wurde, $z_1, z_2, \ldots z_n$ einer Gleichung mit ganzzahligen Coefficienten Genüge leisten, so wird $\varphi(z, \zeta)$ in diesem Falle eine ganze Funktion von z und ζ, also $\varphi(z_i, z_k)$ eine ganze Funktion von z_i, z_k mit ganzzahligen Coefficienten. Da ganz dieselbe Bemerkung sich bezüglich der Grössen $\Phi(z_i, z_k)$ wiederholen lässt, so werden nicht nur die Coefficienten $A, B, \ldots L$ der Gleichungen (27), sondern auch die unter (31) vor. Vorlesung gegebenen Werthe der Grössen $\alpha_i, \beta_i, \ldots \lambda_i$ ganze Funktionen der Wurzeln $z_1, z_2, \ldots z_n$ mit ganzzahligen Coefficienten.

3. Der Keim der Lindemann'schen Betrachtung über die Zahl π ist nun folgende einfache Ueberlegung: Lässt sich zeigen, dass e^ζ nicht rational sein kann, so oft ζ eine algebraische Zahl ist, so folgt aus dem Bestehen der Gleichung $e^{\pi i} = -1$ unmittelbar, dass πi und folglich auch π keine algebraische, also nur eine transcendente Zahl sein kann. — Es genügt aber, hierbei ζ als eine ganze algebraische Zahl anzunehmen. Denn, sei im Gegentheil ζ Wurzel der Gleichung

$$(2) \qquad \zeta^r + p_1\zeta^{r-1} + p_2\zeta^{r-2} + \cdots + p_r = 0$$

mit rationalen Coefficienten, sodass $p_i = \frac{q_i}{q}$ gesetzt werden

kann, unter q, q_i ganze Zahlen, unter q nämlich den Generalnenner aller p_i verstanden, so leistet $\zeta' = q\zeta$ der Gleichung

$$\zeta'^r + Q_1\zeta'^{r-1} + Q_2\zeta'^{r-2} + \cdots + Q_r = 0$$

Genüge, in welcher die Coefficienten $Q_i = q_i q^{i-1}$ sämmtlich ganze Zahlen sind, ist also eine ganze algebraische Zahl. Wird aber e^{ζ} als rational angenommen, so folgt für $e^{\zeta'} = (e^{\zeta})^q$ dasselbe; aus dem Nachweise also, dass $e^{\zeta'}$ nicht rational sein kann, sobald ζ' eine ganze algebraische Zahl ist, folgt dieselbe Unmöglichkeit für e^{ζ}, wenn ζ eine beliebige algebraische Zahl bezeichnet. Hiernach dürfen wir uns im Folgenden auf die Voraussetzung beschränken, dass die Coefficienten der Gleichung (2) ganze Zahlen sind. Auch werden wir offenbar die Allgemeinheit nicht beeinträchtigen, wenn wir jene Gleichung als irreduktibel voraussetzen; denn, wäre die ganze Funktion zur Linken von (2) nicht irreduktibel, so würde sie in irreduktible Faktoren zerlegt werden können, und eine Grösse ζ, welche die Gleichung (2) erfüllt, müsste einen dieser Faktoren zu Null machen und würde daher Wurzel einer ähnlichen irreduktiblen Gleichung sein, welche statt (2) unserer Betrachtung zu Grunde gelegt werden könnte. Bezeichnet man daher mit $\zeta_1, \zeta_2, \ldots \zeta_r$ die Wurzeln der jetzt als irreduktibel anzunehmenden Gleichung (2), so müssen diese bekanntlich alle von einander verschieden sein, weil sonst die ganze Funktion zur Linken mit ihrer Abgeleiteten einen rationalen Faktor gemeinsam haben, also nicht irreduktibel sein würde.

Die Grössen

$$(3) \qquad e^{\zeta_1},\ e^{\zeta_2},\ \ldots\ e^{\zeta_r}$$

sind die Wurzeln der Gleichung

$$(Z - e^{\zeta_1})\cdot(Z - e^{\zeta_2})\cdots(Z - e^{\zeta_r}) = 0$$

d. h., entwickelt geschrieben, der Gleichung r^{ten} Grades

$$(4) \qquad Z^r + M_1 Z^{r-1} + M_2 Z^{r-2} + \cdots + M_r = 0,$$

deren Coefficienten, vom Vorzeichen abgesehen, mit den folgenden Ausdrücken identisch sind:

$$(5) \quad \sum e^{\zeta_1},\quad \sum e^{\zeta_1+\zeta_2},\quad \sum e^{\zeta_1+\zeta_2+\zeta_3},\quad \ldots\quad e^{\zeta_1+\zeta_2+\cdots+\zeta_r}.$$

Hier ist nämlich die erste Summe die Summe der Grössen (3) selbst; die zweite ist die Summe aller Produkte aus zweien von ihnen, d. i. die Summe aller Ausdrücke, welche aus $e^{\zeta_1+\zeta_2}$ entstehen, wenn statt $\zeta_1 + \zeta_2$ die Summe je zweier der Grössen $\zeta_1, \zeta_2, \ldots \zeta_r$ oder die algebraisch verschiedenen Werthe gesetzt werden, welche die Funktion $\zeta_1 + \zeta_2$ von den Wurzeln der Gleichung (2) durch Vertauschung dieser Wurzeln annimmt; u. s. w. Wird nun vorausgesetzt, dass eine der Grössen (3) rational sei, etwa $e^{\zeta_1} = \frac{\mu}{\nu}$, so würde die Gleichung (4), wenn $Z = \frac{\mu}{\nu}$ gesetzt wird, befriedigt und die entstehende Identität würde folgende Gestalt annehmen:

$$(6)\quad N_0 + N_1 \cdot \sum e^{\zeta_1} + N_2 \cdot \sum e^{\zeta_1+\zeta_2} + \cdots + N_r \cdot e^{\zeta_1+\zeta_2+\cdots+\zeta_r} = 0,$$

in welcher $N_0, N_1, N_2, \ldots N_r$ ganze Zahlen bedeuten, welche nicht sämmtlich gleich Null sind; zum Beweise des Lindemann'schen Vorhabens bleibt demnach nur die Unmöglichkeit einer Beziehung dieser Art nachzuweisen.

4. Wir verfolgen hierzu zunächst den Fall, in welchem für jede der in den Exponenten stehenden Wurzelfunktionen $\zeta_1, \zeta_1 + \zeta_2, \zeta_1 + \zeta_2 + \zeta_3, \ldots$ die algebraisch verschiedenen Werthe, welche sie bei den Permutationen der Wurzeln annehmen, auch numerisch von einander verschieden sind. Ist nun

$$F(\zeta_1, \zeta_2, \zeta_3, \ldots \zeta_r)$$

irgend eine ganze Funktion der Wurzeln mit ganzzahligen Coefficienten, so leisten die numerisch verschiedenen Werthe derselben, wie hier als bekannt vorausgesetzt werden muss, einer Gleichung Genüge, welche ebenso wie die gegebene Gleichung (2) ganzzahlige Coefficienten hat und irreduktibel ist. Da hiernach auch die Werthe der Exponenten in jeder der in der Beziehung (6) auftretenden Summen die Wurzeln einer solchen Gleichung sein werden, so kann zunächst keiner aller jener Exponenten Null sein, ausgenommen etwa allein der letzte, $\zeta_1 + \zeta_2 + \zeta_3 + \cdots + \zeta_r$, welcher Null wird, wenn in der Gleichung (2) $p_1 = 0$ wäre. Ferner aber darf man alle

jene Exponenten auch als verschieden von einander voraussetzen, nicht nur die in derselben Summe, was bereits geschehen ist, sondern auch die zu verschiedenen Summen gehörigen; denn, wären zwei solche einander gleich, so müssten die irreduktibeln Gleichungen, denen sie genügen, mit einander identisch sein, also alle Wurzeln gemeinsam haben; dann wären aber jene Summen gleichfalls mit einander identisch und man könnte sie in ein einziges Glied zusammenfassen, ebenso wie in dem vorher erwähnten Falle $p_1 = 0$ das erste und letzte Glied, und erhielte so eine andere Beziehung von ganz ähnlicher Beschaffenheit wie die Beziehung (6), und könnte mit dieser in derselben Weise verfahren wie mit der ursprünglichen, wenn darin alle Exponenten von vornherein als von Null und von einander verschieden vorausgesetzt werden.

Endlich hat irgend welche Vertauschung unter den Wurzeln $\zeta_1, \zeta_2, \dots \zeta_r$ nur die Wirkung, dass in jeder der Summen die Exponenten nur unter einander auf gewisse Weise gleichzeitig vertauscht werden.

Dies vorausgeschickt, setze man

$$(7) \qquad z_1 = \zeta_1, \quad z_2 = \zeta_2, \quad \dots \quad z_r = \zeta_r,$$

bezeichne mit

$$(7) \qquad z_{r+1}, \quad z_{r+2}, \quad \dots \quad z_{r+q}$$

die Werthe, welche die Exponenten der zweiten Summe haben u. s. w., endlich mit

$$(7) \qquad z_n$$

den Exponenten $\zeta_1 + \zeta_2 + \cdots + \zeta_r$ — welcher dem Gesagten zufolge für die anzustellende Betrachtung als von Null verschieden angesehen werden darf —, so sind, wie leicht einzusehen, $z_1, z_2, \dots z_n$ die von Null und von einander verschiedenen Wurzeln einer Gleichung n^{ten} Grades mit ganzzahligen Coefficienten. Die Gleichung (6), deren Unmöglichkeit nachgewiesen werden soll, ist demnach nur ein specieller Fall der Gleichung (32) vor. Vorlesung, und man zieht daraus, ähnlich wie aus jener die Gleichung (33), nachstehende Folgegleichungen:

$$
(8)\quad \begin{cases}
\alpha_0 X_0 + (\alpha_1 + \alpha_2 + \cdots + \alpha_r) X_1 + (\alpha_{r+1} + \cdots + \alpha_{r+\varrho}) X_2 \\
\qquad + \cdots + \alpha_n X_n = \xi_0 \\
\beta_0 X_0 + (\beta_1 + \beta_2 + \cdots + \beta_r) X_1 + (\beta_{r+1} + \cdots + \beta_{r+\varrho}) X_2 \\
\qquad + \cdots + \beta_n X_n = \xi_1 \\
\gamma_0 X_0 + (\gamma_1 + \gamma_2 + \cdots + \gamma_r) X_1 + (\gamma_{r+1} + \cdots + \gamma_{r+\varrho}) X_2 \\
\qquad + \cdots + \gamma_n X_n = \xi_2 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\lambda_0 X_0 + (\lambda_1 + \lambda_2 + \cdots + \lambda_r) X_1 + (\lambda_{r+1} + \cdots + \lambda_{r+\varrho}) X_2 \\
\qquad + \cdots + \lambda_n X_n = \xi_n ,
\end{cases}
$$

in denen zur Abkürzung gesetzt ist:

$$
(9)\quad \xi_0 = \Big[(e^{z_1} \varepsilon^0_{1,m} + \cdots + e^{z_r} \varepsilon^0_{r,m}) X_1 + (e^{z_{r+1}} \varepsilon^0_{r+1,m} + \cdots + e^{z_{r+\varrho}} \varepsilon^0_{r+\varrho,m}) X_2 + \cdots + e^{z_n} \varepsilon^0_{n,m} X_r \Big]
$$

und $\xi_1, \xi_2, \ldots \xi_n$ die entsprechende Bedeutung haben.

5. Vertauscht man nun zwei Grössen z_i, z_k mit einander, welche ein- und derselben der unter (7) unterschiedenen Gruppen von Wurzeln angehören, z. B. z_1 mit z_2, so geht, da allgemein

$$
\varepsilon^h_{i,m} = \frac{1}{1\,.\,2\,.\,3 \ldots (m-1)} \int_{z_0}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z - z_h}\, dz
$$

war, $\varepsilon^h_{1,m}$ in $\varepsilon^h_{2,m}$ und umgekehrt über, wenn h von 1, 2 verschieden ist, während $\varepsilon^h_{g,m}$ dabei unverändert bleibt, wenn auch g weder 1 noch 2 gleich ist. Es geht also z. B.

$$
\varepsilon^0_{1,m} = e^{-z_0} \cdot \alpha_0 - e^{-z_1} \cdot \alpha_1 \quad \text{in} \quad \varepsilon^0_{2,m} = e^{-z_0} \cdot \alpha_0 - e^{-z_2} \cdot \alpha_2
$$

d. h. α_1 in α_2 und umgekehrt über, während

$$
\varepsilon^0_{g,m} = e^{-z_0} \cdot \alpha_0 - e^{-z_g} \cdot \alpha_g
$$

d. h. alle übrigen α ungeändert bleiben, wenn z_1 und z_2 vertauscht werden; bei solcher Vertauschung wird also die linke Seite der ersten Gleichung (8) ungeändert bleiben, ebenso diejenigen der 4ten, 5ten u. s. w., weil diesen die Werthe 3, 4, ... des Index h zukommen würden. Dagegen geht bei derselben Vertauschung

$$\varepsilon^1_{1,m} = \frac{1}{1\,.\,2\,.\,3\,\ldots\,(m-1)} \int_{z_0}^{z_1} e^{-z}\,.\,\frac{f(z)^m}{z-z_1}\,dz$$

in

$$\varepsilon^2_{2,m} = \frac{1}{1\,.\,2\,.\,3\,\ldots\,(m-1)} \int_{z_0}^{z_2} e^{-z}\,.\,\frac{f(z)^m}{z-z_2}\,dz$$

und umgekehrt über, desgleichen $\varepsilon^1_{2,m}$ in $\varepsilon^2_{1,m}$ und umgekehrt, endlich, wenn g von 1 und 2 verschieden ist,

$$\varepsilon^1_{g,m} = \frac{1}{1\,.\,2\,.\,3\,\ldots\,(m-1)} \int_{z_0}^{z_g} e^{-z}\,.\,\frac{f(z)^m}{z-z_1}\,dz$$

in

$$\varepsilon^2_{g,m} = \frac{1}{1\,.\,2\,.\,3\,\ldots\,(m-1)} \int_{z_0}^{z_g} e^{-z}\,.\,\frac{f(z)^m}{z-z_2}\,dz$$

über und umgekehrt; d. h., da

$$\varepsilon^1_{1,m} = e^{-z_0}\beta_0 - e^{-z_1}\beta_1\,,\quad \varepsilon^2_{2,m} = e^{-z_0}\gamma_0 - e^{-z_2}\gamma_2$$
$$\varepsilon^1_{2,m} = e^{-z_0}\beta_0 - e^{-z_2}\beta_2\,,\quad \varepsilon^2_{1,m} = e^{-z_0}\gamma_0 - e^{-z_1}\gamma_1$$
$$\varepsilon^1_{g,m} = e^{-z_0}\beta_0 - e^{-z_g}\beta_g\,,\quad \varepsilon^2_{g,m} = e^{-z_0}\gamma_0 - e^{-z_g}\gamma_g$$

ist, es vertauschen sich, wenn z_1 und z_2 vertauscht werden, gleichzeitig β_0 und γ_0, β_1 und γ_2, β_2 und γ_1, endlich, sobald g von 1, 2 verschieden ist, auch β_g und γ_g. Offenbar wird hierdurch die linke Seite der zweiten Gleichung (8) sich mit derjenigen der dritten vertauschen, da β_1, β_2 bez. γ_1, γ_2 je derselben Summe angehören.

Man findet also im Ganzen: wenn irgend zwei derselben Gruppe (7) angehörige Grössen z_i, z_k vertauscht werden, so ändern sich in den Gleichungen (8) die linken Seiten nicht bis auf zwei, welche mit einander tauschen; und zwar bleibt die linke Seite der ersten jener Gleichungen immer ungeändert, da der ihr entsprechende Werth des Index h, nämlich $h = 0$, immer von i und k verschieden ist. Weil nun jede Permutation der Grössen $z_1, z_2, z_3, \ldots z_n$, bei welcher nur immer solche dieser Grössen unter einander vertauscht werden, welche je derselben Gruppe (7) angehören, durch eine

Reihe Vertauschungen von zwei derselben Gruppe zugehörigen Grössen z_i, z_k hervorgebracht werden kann, gewinnt man sogleich das allgemeinere Ergebniss: Bei jeder der angegebenen Permutationen bleibt die linke Seite der ersten Gleichung (8) ungeändert, diejenigen der anderen aber vertauschen sich nur unter einander.

Nun wissen wir aber schon, dass, wie immer auch die Wurzeln $\zeta_1, \zeta_2, \ldots \zeta_r$ unter einander vertauscht werden mögen, nur solche Vertauschungen zwischen den Grössen $z_1, z_2, \ldots z_n$ daraus hervorgehen, wie sie soeben angegeben wurden. Das gewonnene Ergebniss lässt sich demnach auch so aussprechen: Bei den Vertauschungen der Wurzeln $\zeta_1, \zeta_2, \ldots \zeta_r$ bleibt die linke Seite der ersten Gleichung (8) ungeändert, die n Ausdrücke auf den linken Seiten der übrigen Gleichungen (8) aber vertauschen sich unter einander, und deshalb werden Ausdrücke, welche symmetrisch aus ihnen zusammengesetzt sind, gleichfalls ungeändert bleiben. Beispielsweise, wenn man die Gleichung aufstellte, welche die genannten n Ausdrücke zu Wurzeln hat, so würden die Coefficienten derselben solche symmetrische Ausdrücke sein und würden sich also bei den Vertauschungen der Wurzeln $\zeta_1, \zeta_2, \ldots \zeta_r$ der Gleichung (2) nicht verändern. Nun sind aber die Ausdrücke zur Linken der Gleichungen (8) gemäss der Bedeutung der Zeichen $\alpha, \beta, \gamma, \ldots \lambda$ ganze und ganzzahlige Funktionen der Grössen $z_1, z_2, \ldots z_n$ und demnach auch der Wurzeln $\zeta_1, \zeta_2, \ldots \zeta_r$, und die Coefficienten der Gleichung (2) sind als ganze Zahlen vorausgesetzt worden. Nach den bekanntesten Sätzen über symmetrische Wurzelfunktionen findet sich hieraus endlich, dass die linke Seite der ersten Gleichung (8) einer ganzen Zahl — sie heisse U — gleich, die linken Seiten der n übrigen Gleichungen aber die Wurzeln einer Gleichung n^{ten} Grades

$$(10) \qquad V^n + U_1 \cdot V^{n-1} + U_2 \cdot V^{n-2} + \cdots + U_n = 0$$

sein müssen, deren Coefficienten U_i ebenfalls sämmtlich ganzzahlig sind.

6. Die Gleichungen (8), sowie die aus ihnen gezogenen Folgerungen bestehen für jeden Werth, welchen man m bei-

legen mag, und werden demnach auch bestehen bleiben, wenn wir m unendlich wachsen lassen. Wir wollen untersuchen, was dabei aus den mit $\xi_0, \xi_1, \dots \xi_n$ bezeichneten rechten Seiten jener Gleichungen werden wird. Nun war in dem Integrale

$$(11)\qquad \int_{c}^{z_i} e^{-z} \cdot \frac{f(z)^m}{z - z_h}\, dz$$

der Integrationsweg abgesehen davon, dass er im Endlichen bleiben muss, ein ganz beliebiger; doch wollen wir jetzt übereinkommen, ihn so zu wählen, dass er nicht durch einen der Punkte $z_1, z_2, \dots z_n$ hindurchführe und dass seine Länge, welche l_i^h heisse, nur endlich sei. Auf diesem Wege wird dann nicht nur $f(z)$, sondern auch $\frac{e^{-z}}{z - z_h}$ endliche Werthe behalten, sodass der absolute Betrag jeder dieser Funktionen auf demselben eine obere Grenze haben, nämlich einen endlichen Werth, welcher M_i^h, $M_i'^h$ resp. heissen möge, nicht überschreiten wird. Der absolute Betrag des Integrales (11) wird demnach einem einfachen Principe zufolge auch nicht grösser sein können, als eine leicht angebbare Grösse. Bedenkt man nämlich, dass das Integral, der in No. 2 gegebenen Definition gemäss, nichts anderes ist, als eine Summe von unendlich viel Summanden von der Form

$$\frac{e^{-z}}{z - z_h} \cdot f(z)^m \cdot (z_{\lambda+1} - z_\lambda),$$

so kann infolge des dort hervorgehobenen Satzes sein Modulus nie grösser sein als die Summe der Moduln der einzelnen Summanden, d. i.

$$\sum \mathrm{mod} \cdot \frac{e^{-z}}{z - z_h} \cdot \mathrm{mod} \cdot f(z)^m \cdot \mathrm{mod} \cdot (z_{\lambda+1} - z_\lambda),$$

und umsomehr nicht grösser als

$$\sum M_i^h \cdot (M_i'^h)^m \cdot \mathrm{mod}\,(z_{\lambda+1} - z_\lambda).$$

Hier ist aber $\mathrm{mod}\,(z_{\lambda+1} - z_\lambda)$ gleich dem Abstande der beiden Curvenpunkte z_λ, $z_{\lambda+1}$ von einander d. h. gleich dem Curvenelemente; und da letztere zusammengenommen die ganze Länge

l_i^h des Weges ausmachen, findet sich endlich der absolute Betrag des Integrales nicht grösser als

$$(M_i^h)^m \cdot M_i'^h \cdot l_i^h,$$

also

$$\text{der abs. B. v. } \varepsilon_{i,m}^h < \frac{(M_i^h)^m \cdot M_i'^h \cdot l_i^h}{1 \cdot 2 \cdot 3 \cdots (m-1)}.$$

Bezeichnen also M, M', l die grössten unter den Werthen M_i^h, $M_i'^h$, l_i^h resp., welche allen Combinationen h, i entsprechen, so findet man schliesslich, dass die sämmtlichen Grössen $\varepsilon_{i,m}^h$ ihrem absoluten Betrage nach die Grenze

$$\frac{M^{m-1}}{1 \,.\, 2 \,.\, 3 \ldots (m-1)} \cdot M M' l$$

nicht überschreiten. Hierbei sind M, M', l Werthe, welche von m unabhängig sind, und demnach sinkt die bezeichnete Grenze wegen ihres ersten Faktors mit unendlich wachsendem m schliesslich unter jeden Grad von Kleinheit herab. Gleiches wird demnach auch mit dem absoluten Betrage der Grössen $\varepsilon_{i,m}^h$ und Gleiches also auch mit demjenigen der Grössen ξ_0, ξ_1, ξ_2, ... ξ_n geschehen: für alle m, welche eine gewisse Zahl μ übertreffen, wird der absolute Betrag dieser Grössen beliebig klein sein, z. B. derjenige von ξ_0 kleiner als Eins. Da aber die linke Seite der ersten der Gleichungen (8), welche gleich ξ_0 war, immer eine ganze Zahl ist, muss für alle $m > \mu$ ihr Werth die Null sein.

Die linken Seiten der übrigen n Gleichungen (8) waren aber die Wurzeln der Gleichung (10); da nach dem Gesagten diese Wurzeln sämmtlich nach ihrem absoluten Betrage beliebig klein werden, sobald $m > \mu$ ist, muss das Gleiche auch gelten von ihren Coefficienten U_1, U_2, ... U_n; diese letzteren werden z. B., μ hinreichend gross gewählt, sämmtlich kleiner als Eins und folglich, da sie ganze Zahlen bedeuten, sämmtlich gleich Null sein müssen. Dann sind es aber auch die Wurzeln der Gleichung (10) selbst, d. h. die linken Seiten der Gleichungen (8). Man findet also im Ganzen, dass für alle hinreichend grossen Werthe von m die Gleichungen stattfinden:

$$\alpha_0 N_0 + (\alpha_1 + \alpha_2 + \cdots + \alpha_r) N_1 + (\alpha_{r+1} + \cdots + \alpha_{r+\varrho}) N_2 + \cdots + \alpha_n N_r = 0$$

$$\beta_0 N_0 + (\beta_1 + \beta_2 + \cdots + \beta_r) N_1 + (\beta_{r+1} + \cdots + \beta_{r+\varrho}) N_2 + \cdots + \beta_n N_r = 0$$

. . . .

$$\lambda_0 N_0 + (\lambda_1 + \lambda_2 + \cdots + \lambda_r) N_1 + (\lambda_{r+1} + \cdots + \lambda_{r+\varrho}) N_2 + \cdots + \lambda_n N_r = 0,$$

welche doch nur stattfinden können, da die N_i nicht sämmtlich Null sein sollten, wenn die aus den Grössen α_i, β_i, γ_i, ... λ_i gebildete Determinante verschwindet. Dies kann aber nur geschehen, wie gelegentlich der Zahl e gezeigt ist, wenn die Discriminante der Gleichung mit den Wurzeln $z_1, z_2, \ldots z_n$ verschwindet, und geschieht also nicht, wenn diese Grössen, wie hier vorausgesetzt werden durfte, von einander verschieden sind.

Hiermit ist die Unmöglichkeit der Beziehung (6) unter der am Anfange von No. 4 gemachten Annahme erwiesen.

Wir müssten nunmehr auch den Fall erledigen, wo die algebraisch verschiedenen Werthe der Wurzelfunktionen $\zeta_1 + \zeta_2$, $\zeta_1 + \zeta_2 + \zeta_3$, ..., welche in der Gleichung (6) als Exponenten sich finden, nicht sämmtlich auch numerisch ungleich sind. Dann erst wäre der Beweis für die Transcendenz der Zahl π vollständig erbracht. Dieser Theil der Lindemann'schen Untersuchung bietet nun aber gewisse Schwierigkeiten dar, insofern er eine weitere Bekanntschaft mit dem Verhalten der Wurzelfunktionen bei Vertauschung der Wurzeln erfordert, als hier für bekannt angenommen werden soll; deshalb, und weil durch das bereits Gesagte die Art und Weise jener Untersuchung genügend gekennzeichnet worden ist, ziehe ich es vor, den zu leistenden Beweis auf einem einfacheren Wege zu erbringen, nämlich statt der Lindemann'schen Darstellung noch in Kürze den wesentlichsten Inhalt der Abhandlung mitzutheilen, in welcher Weierstrass dieselbe zu vereinfachen gesucht und gelehrt hat.

Neunte Vorlesung.

Weierstrass' Beweis von der Transcendenz der Zahl π.

1. Weierstrass begründet seinen Beweis für die Transcendenz der Zahl π auf einen Hilfssatz, zu dessen Herleitung ihm die Hermite'sche Untersuchung über die Zahl e den Weg angegeben hat. Direkter als er selbst es gethan hat, wollen wir hier mit unserer Betrachtung an jene Untersuchung anknüpfen, indem wir zu der Formel (24) der 6. Vorlesung zurückkehren. Wir wählen darin $x = 1$ und erhalten die Gleichung

$$(1) \qquad \int e^{-z} \cdot F(z)\, dz = -\, e^{-z} \cdot \mathfrak{F}(z),$$

worin

$$(2) \qquad \mathfrak{F}(z) = F(z) + F'(z) + \cdots + F^{(\mu)}(z),$$

μ aber der Grad der ganzen Funktion $F(z)$ ist. Nun seien

$$(3) \qquad \begin{cases} f(z) = a_0 z^{n+1} + a_1 z^n + \cdots + a_n z + a_{n+1} \\ h(z) = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_0 \end{cases}$$

ganze Funktionen $n+1^{\text{ten}}$ bez. n^{ten} Grades, deren erstere lauter ungleiche Wurzeln haben soll, während die Coefficienten der letztern ganz willkürlich sind; und man wähle nun

$$(4) \qquad F(z) = \frac{h(z) \cdot f(z)^m}{m!}.$$

Bei dieser Wahl findet sich

$$F'(z) = \frac{h'(z) f(z)^m}{m!} + \frac{h(z) \cdot f(z)^{m-1} \cdot f'(z)}{(m-1)!}$$

$$F''(z) = \frac{h''(z) f(z)^m}{m!} + 2\, \frac{h'(z) \cdot f(z)^{m-1} \cdot f'(z)}{(m-1)!}$$

$$+ \frac{h(z) \cdot f(z)^{m-2} \cdot f'(z)^2}{(m-2)!} + \frac{h(z) \cdot f(z)^{m-1} \cdot f''(z)}{(m-1)!}$$

u. s. w. Man kann demnach $\mathfrak{F}(z)$ nach den fallenden Potenzen von $f(z)$ geordnet denken, und, wenn man so

$$(5) \qquad \mathfrak{F}(z) = \frac{H_0(z)}{m!} f(z)^m + \frac{H_1(z)}{(m-1)!} f(z)^{m-1} + \cdots$$

$$+ H_{m-1}(z) \cdot f(z) + H_m(z)$$

kürzer

$$(6)\qquad \mathfrak{F}(z) = \sum_{i=0}^{m} \frac{H_i(z)}{(m-i)!} \cdot f(z)^{m-i}$$

setzt, so sind ersichtlich die Funktionen $H_i(z)$ ganze und ganzzahlige Funktionen der Grössen z, a_0, a_1, ... a_{n+1}, c_0, c_1, ... c_n und zwar homogene lineare Funktionen der letztgenannten Coefficienten c_0, c_1, ... c_n. Aus der Grundformel (1) folgt mit Rücksicht auf (4)

$$\frac{h(z)\, f(z)^m}{m!} = \mathfrak{F}(z) - \mathfrak{F}'(z).$$

Wenn also die c_i nicht sämmtlich Null sind, so ist $\mathfrak{F}(z)$ eine ganze Funktion vom Grade $\mu = n + m(n+1)$, welche nicht für jeden Werth von z verschwindet; die vorige Gleichung lehrt zudem, dass $\mathfrak{F}(z)$ nicht durch $f(z)$ theilbar ist. Denn, wäre sie es im Gegentheil, und setzte man dann

$$\mathfrak{F}(z) = \varphi(z) \cdot f(z)^{\varrho},$$

worin $\varphi(z)$ nun nicht mehr durch $f(z)$ theilbar gedacht wird, so fände sich nach jener Gleichung

$$\left(\varphi(z) - \varphi'(z)\right) \cdot f(z) - \varrho \cdot \varphi(z) f'(z) = \frac{h(z) \cdot f(z)^{m-\varrho+1}}{m!};$$

also müsste $\varrho \cdot \varphi(z) f'(z)$ durch $f(z)$ theilbar sein; nach der über die Wurzeln von $f(z)$ gemachten Voraussetzung hat aber $f'(z)$ keinen Theiler gemeinsam mit $f(z)$ und $\varphi(z)$ ist nicht theilbar durch $f(z)$; man kommt also auf einen Widerspruch, sobald man ϱ von Null verschieden d. h. die Funktion $\mathfrak{F}(z)$ in der That theilbar durch $f(z)$ voraussetzt; da hiernach $\mathfrak{F}(z)$ nicht durch $f(z)$ theilbar sein kann, so ist es nach (5) die Funktion $H_m(z)$ ebensowenig.

2. So oft z irgend einen der Werthe bedeutet, für welche $f(z)$ verschwindet, reducirt sich nach (5) $\mathfrak{F}(z)$ auf $H_m(z)$. Sind demnach z', z'' zwei Wurzeln der Gleichung $f(z) = 0$, und integrirt man in der Formel (1) auf irgend einem Wege zwischen den Werthen z', z'', so findet man die Gleichung

$$(7)\qquad H_m(z'') \cdot e^{-z''} - H_m(z') \cdot e^{-z'} = -\int_{z'}^{z''} \frac{f(z)^m\, h(z)}{m!}\, e^{-z}\, dz.$$

Die obigen Ausdrücke für $F'(z)$, $F''(z)$, ... aber zeigen, dass das erste durch $f(z)$ nicht theilbare Glied von $\mathfrak{F}(z)$ aus $F^{(m)}(z)$ hervorgeht, in dessen Ausdrucke das Glied $h(z)f'(z)^m$ sich findet; $H_m(z)$ ist demnach von demselben Grade, wie dieses Glied, nämlich vom Grade $(m+1)n$; zudem erkennt man aus der Zusammensetzung der einzelnen Glieder jener Ausdrücke, dass die höchsten Coefficienten von $H_m(z)$ nach der Reihe durch a_0^m, a_0^{m-1}, ... a_0 theilbar sein müssen; daraus folgt, dass die Funktion $a_0^{m(n-1)} \cdot H_m(z)$ sich auf die Form

$$(8) \qquad a_0^{m(n-1)} \cdot H_m(z) = G(z,m) \cdot f(z) + g(z,m)$$

bringen lässt, worin $G(z,m)$, $g(z,m)$ beides ganze und ganzzahlige Funktionen der Grössen z, a_0, a_1, ... a_{n+1}, c_0, c_1, ... c_n, die letztere höchstens vom Grade n in Bezug auf z bedeuten. Und damit nimmt die Gleichung (7) folgende einfachere Gestalt an:

$$(9) \qquad \begin{aligned} & g(z'',m) \cdot e^{-z''} - g(z',m) \cdot e^{-z'} \\ & = -\int_{z'}^{z''} h(z) \frac{\left(a_0^{n-1} f(z)\right)^m}{m!} e^{-z}\, dz. \end{aligned}$$

Die Funktionen $G(z,m)$ bez. $g(z,m)$ sind, ebenso wie $H_m(z)$, homogene lineare Funktionen der Coefficienten c_i. Man kann demnach

$$(10) \quad G(z,m) = \sum_{i=0}^{n} c_i G_i(z,m), \quad g(z,m) = \sum_{i=0}^{n} c_i \cdot g_i(z,m)$$

setzen, indem man unter $G_i(z,m)$, $g_i(z,m)$ diejenigen Ausdrücke versteht, welche jene allgemeinen Funktionen annehmen, wenn $c_i = 1$, alle übrigen c gleich Null gewählt werden, d. h. wenn $h(z)$ sich auf z^i reducirt. Demnach liefert die eine Gleichung (9) folgende $n+1$ Gleichungen:

$$(11) \qquad \begin{aligned} & g_i(z'',m) \cdot e^{-z''} - g_i(z',m) \cdot e^{-z'} \\ & = -\int_{z'}^{z''} z^i \cdot \frac{\left(a_0^{n-1} f(z)\right)^m}{m!} e^{-z}\, dz \end{aligned}$$

(für $i = 0, 1, 2 \cdots n$)

und die Gleichung (8) nimmt die Gestalt an:

$$a_0^{m(n-1)} \cdot H_m(z) = f(z) \cdot \sum_{i=0}^{n} c_i \cdot G_i(z, m) + \sum_{i=0}^{n} c_i \cdot g_i(z, m)$$

und lehrt zufolge dem zuvor bewiesenen Umstande, dass $H_m(z)$ nicht durch $f(z)$ theilbar ist, dass der Ausdruck

$$\sum_{i=0}^{n} c_i \cdot g_i(z, m) \tag{12}$$

nicht für jeden Werth von z gleich Null sein kann.

Bedeuten also $z_0, z_1, z_2, \ldots z_n$ $n+1$ ungleiche Werthe, so hat die Determinante der Grössen $g_i(z_k, m)$, nämlich:

$$\Gamma = \begin{vmatrix} g_0(z_0, m), & g_1(z_0, m), & \ldots & g_n(z_0, m) \\ g_0(z_1, m), & g_1(z_1, m), & \ldots & g_n(z_1, m) \\ \cdot & \cdot & \cdot & \cdot \\ g_0(z_n, m), & g_1(z_n, m), & \ldots & g_n(z_n, m) \end{vmatrix} \tag{13}$$

stets einen von Null verschiedenen Werth. Denn sonst könnten die $n+1$ Gleichungen

$$\sum_{i=0}^{n} c_i \cdot g_i(z_k, m) = 0$$

$$(\text{für } k = 0, 1, 2, \cdots n)$$

mit einander bestehen, ohne dass die $n+1$ Grössen $c_0, c_1, \ldots c_n$ sämmtlich Null wären; das heisst aber: der Ausdruck (12), welcher eine ganze Funktion von z höchstens vom Grade n ist, würde für mehr als n Werthe von z und daher — zuwider dem soeben Bewiesenen — für jedes z gleich Null sein.

Diese Ergebnisse, insbesondere die Formel (11), haben Giltigkeit, wie gross die mit m bezeichnete ganze Zahl auch gedacht werde; man kann letztere aber so gross wählen, dass die rechte Seite der Gleichung (11) ihrem absoluten Betrage nach beliebig klein wird. In der That, wenn der beliebige Integrationsweg jetzt als ein endlicher und seine Länge gleich l vorgestellt wird, so heisse M der grösste absolute Betrag, welchen $z^i e^{-z}$ längs des Integrationsweges annimmt, M' das Maximum des absoluten Betrages von $a_0^{n-1} f(z)$ längs desselben. Dann ist — ähnlich wie in No. 6 der vor. Vorlesung — der

absolute Betrag des Integrales kleiner als $M \cdot \frac{M'^m}{m!} \cdot l$ und sinkt mit wachsendem m zugleich mit dem zweiten Faktor dieses Produkts unter jeden Grad von Kleinheit herab. Also convergirt auch die linke Seite der Gleichung (11), oder auch, nachdem sie mit $e^{z'+z''}$ multiplicirt ist, der Ausdruck

$$(14) \qquad g_i(z', m) \cdot e^{z''} - g_i(z'', m) \cdot e^{z'}$$

bei unendlich wachsendem m gegen Null.

3. Wir verstehen nunmehr unter $z_0, z_1, \ldots z_n$ sämmtliche Wurzeln der Gleichung $f(z) = 0$, die wir als ungleich bereits vorausgesetzt hatten, und nehmen ausserdem jetzt an, dass die Coefficienten in dieser Gleichung ganze Zahlen sind. Entsprechend werden dann, dem oben schon Gesagten gemäss, auch die Coefficienten der Funktionen $g_i(z, m)$ sämmtlich ganzzahlig sein. Nach der vorigen Nummer ist ferner die Determinante Γ von Null verschieden und m kann so gross gewählt werden, dass jede der Grössen

$$g_i(z_0, m) \cdot e^{z_k} - g_i(z_k, m) \cdot e^{z_0}$$
$$(\text{für } i, k = 0, 1, 2 \cdots n)$$

ihrem absoluten Betrage nach kleiner ist, als eine beliebig klein angenommene positive Zahl δ.

Hiermit ist der Hilfssatz von Weierstrass bewiesen und kann folgendermassen ausgesprochen werden:

Es sei $f(z)$ eine ganze und ganzzahlige Funktion $n + 1^{\text{ten}}$ Grades von z mit den von einander verschiedenen Wurzeln $z_0, z_1, z_2, \ldots z_n$, so giebt es ein System

$$g_0(z),\ g_1(z),\ \ldots\ g_n(z)$$

von $n + 1$ ganzen und ganzzahligen Funktionen von z, höchstens vom Grade n, so beschaffen, dass die Determinante der Grössen $g_i(z_k)$ von Null verschieden und jede der Differenzen

$$g_i(z_0) \cdot e^{z_k} - g_i(z_k) \cdot e^{z_0}$$
$$(\text{für } i, k = 0, 1, 2, \cdots n)$$

ihrem absoluten Betrage nach kleiner ist, als eine beliebig klein angenommene positive Zahl δ.

4. Auf Grund dieses Satzes lässt sich nun der Nachweis für die Transcendenz der Zahl π folgendermassen erbringen.

Bekanntlich hat die Gleichung $e^x + 1 = 0$ keine andern Lösungen, als die durch die Formel

$$x = (2n + 1)\pi i \tag{15}$$

gegebenen Werthe von x. Lässt sich demnach zeigen, dass der Ausdruck $e^x + 1$ einen von Null verschiedenen Werth hat, sobald x eine *algebraische* Zahl ist, so folgt sogleich, dass jeder durch die Formel (15) gegebene Werth und damit auch die Zahl π eine nicht algebraische Zahl sein muss. Alles läuft also darauf hinaus, jenen Nachweis zu führen.

Es bedeute zu diesem Zwecke

$$x^r + C_1 x^{r-1} + C_2 x^{r-2} + \cdots + C_r = 0 \tag{16}$$

eine beliebige Gleichung mit rationalen Coefficienten und von einem Grade $r > 2$; ihre Wurzeln, welche, ohne die Allgemeinheit zu beschränken, als ungleich vorausgesetzt werden dürfen, seien $x_1, x_2, x_3, \ldots x_r$. Betrachten wir das Produkt

$$\prod_{h=1}^{r} (e^{x_h} + 1) = (e^{x_1} + 1)(e^{x_2} + 1) \cdots (e^{x_r} + 1)$$

und daneben das gleichgebildete Produkt

$$\prod_{h=1}^{r} (e^{\xi_h} + 1) = (e^{\xi_1} + 1)(e^{\xi_2} + 1) \cdots (e^{\xi_r} + 1),$$

in welchem $\xi_1, \xi_2, \ldots \xi_r$ beliebige Unbestimmte bezeichnen. Das allgemeine Glied des entwickelten Produktes kann man schreiben:

$$e^{\varepsilon_1 \xi_1 + \varepsilon_2 \xi_2 + \cdots + \varepsilon_r \xi_r},$$

wo die ε_i entweder 0 oder 1 sind, und man erhält offenbar alle Glieder, wenn man für die ε_i alle möglichen Combinationen dieser zwei Werthe allmählich einsetzt, sodass man setzen kann:

$$\prod_{h=1}^{r} (e^{\xi_h} + 1) = \sum e^{\varepsilon_1 \xi_1 + \varepsilon_2 \xi_2 + \cdots + \varepsilon_r \xi_r}.$$

wo die r-fache Summation sich eben auf alle diese Combinationen erstreckt, also $p = 2^r$ Summanden vorhanden sein werden. Die Exponenten in dieser Summe, in irgend einer Anordnung genommen, seien $\zeta_0, \zeta_1, \zeta_2, \ldots \zeta_{p-1}$, sodass

$$\prod_{h=1}^{r} (e^{\xi_h} + 1) = \sum_{k=0}^{p-1} e^{\zeta_k}. \tag{17}$$

Sind $z_0, z_1, z_2, \ldots z_{p-1}$ die Werthe, welche $\zeta_0, \zeta_1, \zeta_2, \ldots \zeta_{p-1}$ dadurch annehmen, dass man den Unbestimmten $\xi_1, \xi_2, \ldots \xi_r$ die bestimmten Werthe $x_1, x_2, \ldots x_r$ beilegt, so ergiebt sich aus (17) sogleich auch

$$\prod_{h=1}^{r} (e^{x_h} + 1) = \sum_{k=0}^{p-1} e^{z_k}. \tag{18}$$

Die Anzahl der von einander verschiedenen Werthe, welche in der Reihe $z_0, z_1, z_2, \ldots z_{p-1}$ vorhanden sind, sei $n + 1$; da unter diesen Werthen, indem man alle ε_i bis auf eins, das gleich 1 ist, gleich 0 wählt, auch die Wurzeln $x_1, x_2, \ldots x_r$ gefunden werden, ist $n + 1$ sicher grösser als 1; die Ausdrücke $\zeta_0, \zeta_1, \zeta_2, \ldots \zeta_{p-1}$ können dabei so geordnet gedacht werden, dass die Grössen $z_0, z_1, z_2, \ldots z_n$ die unter einander verschiedenen z_i darstellen und $z_0 = 0$ ist. Dies vorausgesetzt, lässt sich nun eine ganze und ganzzahlige Funktion $f(z)$ vom Grade $n + 1$ angeben, welche diese $n + 1$ Werthe $z_0, z_1, z_2, \ldots z_n$ zu Wurzeln hat.

Betrachtet man nämlich das Produkt

$$\prod_{k=0}^{p-1} (z - \zeta_k) = \prod (z - \varepsilon_1 \xi_1 - \varepsilon_2 \xi_2 - \cdots - \varepsilon_r \xi_r),$$

das letztere über alle p Combinationen erstreckt, welche den Werthen $\varepsilon_i = 0, 1$ entsprechen, so ist dasselbe offenbar eine ganze und ganzzahlige Funktion der Grössen $z, \xi_1, \xi_2, \ldots \xi_r$, welche in Bezug auf die ξ_i symmetrisch ist. Erhalten also die Unbestimmten ξ_i jetzt die Bedeutung als Wurzeln x_i der Gleichung (16), so wird das Produkt

$$\prod_{k=0}^{p-1} (z - z_k)$$

eine ganze Funktion von z sein, deren Coefficienten ganze und ganzzahlige symmetrische Funktionen von diesen Wurzeln und folglich ganze und ganzzahlige Funktionen von den Coefficienten der algebraischen Gleichung sind; haben diese rationale Werthe, wie wir es von der Gleichung (16) vorausgesetzt haben, so wird demnach jenes Produkt eine ganze Funktion von z sein mit gleichfalls rationalen Coefficienten. Wir denken uns diese ganze Funktion — sie heisse $\psi(z)$ — durch den grössten gemeinsamen Theiler dividirt, den sie mit ihrer ersten Abgeleiteten $\psi'(z)$ gemeinsam hat; der Quotient hat bekanntlich gleichfalls rationale Coefficienten, aber nur noch die von einander verschiedenen z_k, d. h. die Werthe $z_0, z_1, z_2, \ldots z_n$ zu Wurzeln; mit dem Generalnenner der rationalen Coefficienten multiplicirt wird er also eine ganze Funktion $f(z)$ $n+1^{\text{ten}}$ Grades mit ganzzahligen Coefficienten sein, welche jene Werthe zu Wurzeln hat, eine Funktion also, wie sie nachgewiesen werden sollte.

5. Nunmehr findet der Hilfssatz von Weierstrass seine Verwendung. Denn in Anwendung auf die soeben festgestellte Funktion $f(z)$ ergiebt er das Vorhandensein von $n+1$ ganzen Funktionen $g_0(z), g_1(z), \ldots g_n(z)$ von der im Hilfssatze angegebenen Beschaffenheit, der Art insbesondere, dass, wenn δ ein beliebig kleiner positiver Werth ist, die sämmtlichen Ausdrücke

$$g_i(0) \cdot e^{z_k} - g_i(z_k)$$

ihrem absoluten Betrage nach kleiner als δ sind, oder, was dasselbe sagt, dass

$$g_i(0) \cdot e^{z_k} - g_i(z_k) = \varepsilon_{i,k} \cdot \delta$$

gesetzt werden kann, während die absoluten Beträge von $\varepsilon_{i,k}$ sämmtlich kleiner als 1 sind, die Determinante der Grössen $g_i(z_k)$ aber von Null verschieden ist. Wir wollen sogleich δ so klein gewählt denken, dass $p \cdot a_0^n \cdot \delta < 1$ ist. In der vorstehenden Gleichung erhält zwar k mit Bezug auf den Hilfssatz nur die Werthe $0, 1, 2, \ldots n$, welche auch i erhält; aber, da die übrigen z_i der Reihe $z_0, z_1, z_2, \ldots z_{p-1}$ keine andern Werthe als einen der Reihe $z_0, z_1, \ldots z_n$ darstellen, so darf man k die ganze Reihe $0, 1, 2, \ldots p-1$ durchlaufen lassen.

So findet man durch Summation aus jener Gleichung zunächst die andere:

$$a_0^n g_i(0) \cdot \sum_{k=0}^{p-1} e^{z_k} = \sum_{k=0}^{p-1} a_0^n g_i(z_k) + \delta \cdot a_0^n \cdot \sum_{k=0}^{p-1} \varepsilon_{i,k}$$

oder, da der absolute Betrag der letztern Summe nicht grösser als p sein kann, diese folgende:

$$(19) \qquad a_0^n g_i(0) \cdot \sum_{k=0}^{p-1} e^{z_k} = \sum_{k=0}^{p-1} a_0^n g_i(z_k) + \eta_i, \qquad (\text{für } i = 0, 1, 2 \cdots n)$$

worin der absolute Betrag von η_i kleiner als 1 ist.

Zur besseren Erkenntniss der Natur der Summe auf der Rechten dieser Gleichung betrachten wir zunächst die ähnliche Summe

$$\sum_{\kappa=0}^{p-1} a_0^n \cdot g_i(\zeta_\kappa) = \sum a_0^n \cdot g_i(\varepsilon_0 \xi_0 + \varepsilon_1 \xi_1 + \cdots + \varepsilon_r \xi_r),$$

letztere Summe über alle Combinationen der Werthe $\varepsilon_i = 0, 1$ erstreckt. Da g_i eine ganze und ganzzahlige Funktion bedeutet, ist auch diese Summe eine ganze und ganzzahlige Funktion der Grössen $\xi_1, \xi_2, \ldots \xi_r$, aber in Beziehung auf dieselben offenbar auch symmetrisch; demnach ist

$$(20) \qquad \sum_{k=0}^{p-1} a_0^n \cdot g_i(z_k)$$

eine ganze und ganzzahlige symmetrische Funktion der Grössen $x_1, x_2, \ldots x_r$ d. h. der Wurzeln von (16), also eine ganze und ganzzahlige Funktion der Coefficienten dieser Gleichung und daher jedenfalls eine rationale Zahl. Andererseits ist g_i eine ganze und ganzzahlige Funktion höchstens vom n^{ten} Grade, und demnach hat $a_0^n g_i(z_k)$ die allgemeine Gestalt

$$A_0 (a_0 z_k)^n + A_1 (a_0 z_k)^{n-1} + \cdots + A_{n-1} \cdot a_0 z_k + A_n,$$

worin die A_i ganze Zahlen sind. Da nun z_k als Wurzel der Gleichung $f(z) = 0$ eine ganze algebraische Zahl ist, so ist's auch $a_0 z_k$ und — nach dem Zusatze in No. 2 der 2. Vorlesung — auch der vorstehende Ausdruck und folglich auch

die ganze Summe (20). Eine ganze algebraische Zahl aber, welche rational ist, ist (s. Vorlesung 1 No. 2) sogar eine ganze Zahl, und so gewinnen wir, alles in allem, das Ergebniss: die Summe (20) ist gleich einer gewöhnlichen *ganzen* Zahl.

Aber diese ganze Zahl kann nicht für *jeden* der Werthe $i = 0, 1, 2, \ldots n$ gleich Null sein. Denn, indem man in der Summe (20) diejenigen Glieder zusammennimmt, in denen z_k denselben Werth hat, kann sie gesetzt werden gleich:

$$\sum_{k=0}^{n} N_k \cdot g_i(z_k),$$

(für $i = 0, 1, 2, \cdots n$)

worin nun die N_k sämmtlich positive ganze Zahlen bedeuten; und diese $n + 1$ Ausdrücke können nicht sämmtlich verschwinden, da es sonst auch ihre Determinante, nämlich die Determinante Γ, müsste, dem Hilfssatze von Weierstrass zuwider.

Es giebt also sicher wenigstens einen Werth von i, für welchen in (19) das erste Glied rechts eine von Null verschiedene ganze Zahl und demnach die ganze rechte Seite nicht Null ist. Für diesen Werth von i wird dann auch die linke Seite d. h. nach (18) das Produkt

$$a_0^n g_i(0) \cdot \prod_{h=1}^{r} (e^{x_h} + 1)$$

von Null verschieden sein, und demnach kann keiner der Faktoren $e^{x_h} + 1$ gleich Null sein, d. h. $e^x + 1$ ist stets von Null verschieden, wenn x eine algebraische Zahl ist; denn x_h, als Wurzel der Gleichung (16) vorausgesetzt, bedeutet jede beliebige algebraische Zahl. In der That, die scheinbare Beschränkung, der wir die Gleichung (16) unterwarfen, indem wir ihren Grad mindestens gleich 2 voraussetzten, hindert nicht, jenen Satz auszusprechen; wäre nämlich x Wurzel einer Gleichung ersten Grades mit rationalen Coefficienten, so wär's selbst eine rationale Zahl; e^x aber ist für ein rationales x stets positiv und demnach kann auch in diesem Falle $e^x + 1$ nicht Null sein.

6. So ist — wie man sieht, durch Betrachtungen von verhältnissmässiger Einfachheit — die wichtige Erkenntniss strenge begründet, dass die Zahl π eine nicht algebraische Zahl ist. Zugleich hiermit ist nun aber eine Frage endlich auf entscheidende Weise beantwortet, über eine Aufgabe endgiltig entschieden worden, welche viele Jahrhunderte lang eine offene gewesen ist und hundertfältige Versuche der Lösung veranlasst hat. Freilich entsprangen diese letztern zum grossen Theile der missverstehenden Auffassung Unberufener. Es handelt sich um das weltberühmte Problem von der Quadratur des Kreises d. i. um die Aufgabe: ein Quadrat zu bestimmen, dessen Inhalt gleich demjenigen eines gegebenen Kreises ist. Ein Kreis aber ist nach seiner Grösse gegeben, wenn sein Radius gegeben wird; und die Aufgabe, richtig verstanden, würde verlangen: es soll eine Construktion gefunden werden, welche aus dem gegebenen Kreisradius die Seite jenes Quadrates ermittelt. Die alte Geometrie, welche zuerst diese Aufgabe sich stellte, kannte keine andern Hilfsmittel der geometrischen Construktion, als den Zirkel und das Lineal, d. h., richtiger gesagt, Kreislinie und Gerade. Und so würde das Problem von der Quadratur des Kreises, noch genauer ausgesprochen, folgendermassen zu fassen sein: Aus dem gegebenen Kreisradius — welcher dabei als Längeneinheit gewählt werden darf — soll durch eine geometrische Construktion, bei welcher nur Gerade und Kreislinien zur Verwendung kommen, die Seite eines Quadrates gefunden werden, dessen Inhalt demjenigen des Kreises gleich ist.

Die Versuche der Mathematiker, diese Aufgabe zu lösen, haben sich nun allezeit als vergeblich erwiesen; obwohl die mathematische Wissenschaft nach verschiedensten Seiten hin die ausserordentlichsten Fortschritte machte, brachten doch diese Fortschritte, auch der geometrischen Disciplinen, nicht den geringsten Gesichtspunkt herbei, unter welchem die Lösung der Aufgabe zu erhoffen war, und so waren die Mathematiker seit lange von der Unmöglichkeit derselben überzeugt und hatten sich darein gefunden, eine Entscheidung darüber dem stetigen Entwicklungsgange der Wissenschaft zu über-

lassen. Denn mehr als einmal ist es geschehen, dass durch den letztern zwischen Problemen, welche ganz verschiedenen Gebieten der Mathematik angehören, eine unerwartete Beziehung aufgedeckt worden ist und dann eine Aufgabe, welche mit den Hilfsmitteln der einen Disciplin nicht gelöst werden konnte, in einer andern ihre Erledigung fand. Mancher freilich, der ausserhalb der Wissenschaft stand, glaubte sich befähigt, die Frage mit den Kenntnissen, die er von der Schule her gerettet, angreifen und lösen zu können, wobei es mit der mathematischen Strenge der Lösung oft genug nicht genau genommen und, wie Kummer einmal es ausgedrückt hat, allerlei Mittel angewandt wurden, nur dasjenige nicht, was in der Mathematik einzig zum Ziele führt, der Verstand. Die Akademien, welche mit der Prüfung solcher Lösungen bemüht wurden, sahen sich schliesslich zu dem Beschlusse genöthigt, gegenüber jedem neuen Versuche dieser Art sich ablehnend zu verhalten. Wie richtig die Wissenschaft gethan, sich eine Zeit lang zu bescheiden, zeigt nun die jetzt gewonnene Entscheidung; in der That: wieder nicht durch gewaltsame Versuche in der nächstliegenden Wissenschaft, der Geometrie, sondern aus einer ganz anderen Quelle, die erst mit den Fortschritten einer viel jüngeren Disciplin, der Algebra, eröffnet worden ist, wurde es möglich, die Erkenntniss zu gewinnen, dass die Quadratur des Kreises eine Unmöglicheit, nämlich die genannte Aufgabe unlösbar ist.

Man kann die geometrische Fassung unserer Aufgabe in der That leicht durch eine algebraische ersetzen, wenn man sich erinnert, dass die Construktion von geradlinigen Strecken mittels Geraden und Kreislinien im wesentlichen nur auf eine der beiden Aufgaben zurückkommt: 1) zu drei gegebenen Strecken die vierte Proportionale, 2) zu zwei gegebenen Strecken die mittlere Proportionale zu finden; d. h. arithmetisch aufgefasst: eine Grösse x durch die Gleichung $\frac{x}{a} = \frac{b}{c}$ bez. durch die Gleichung $\frac{x}{a} = \frac{b}{x}$ oder $x^2 = ab$ zu ermitteln. Dies sind algebraische Gleichungen ersten bez. zweiten Grades. Wenn demnach eine gewisse Strecke aus einer oder mehreren gegebenen Strecken, z. B. die Quadratseite aus dem gegebenen

Kreisradius, mittels Zirkel und Lineal d. h. durch eine gewisse Reihe von Construktionen der genannten beiden Arten construirbar sein soll, so muss ihre Grösse ermittelt werden können, indem man eine entsprechende Reihe von algebraischen Gleichungen der angegebenen Art löst und verknüpft. Die gesuchte Grösse entsteht mit andern Worten aus der Gegebenen mittels einer Reihenfolge rationaler Operationen und Wurzelausziehungen, sodass, wie leicht einzusehen ist, eine gewisse algebraische Gleichung hergestellt werden kann, welcher sie genügt. Ihr Werth wäre demnach — mit Benutzung des von uns eingeführten Ausdrucks — eine algebraische Zahl. Ist nun aber die Seite jenes Quadrates eine solche, so ist's auch der Inhalt des Quadrates, welcher, wenn er dem Inhalte des Kreises vom Radius r gleich sein soll, bekanntlich durch πr^2 oder, falls wir den Kreisradius zur Längeneinheit wählen, durch die Zahl π gemessen wird. Diese müsste also, wäre die Quadratur des Kreises möglich, eine algebraische Zahl sein; da wir sie als eine nicht algebraische erkannt haben, ist die Quadratur des Kreises unmöglich.

So ist es das rühmliche Verdienst des Herrn Lindemann, indem er uns die an sich höchst interessante Erkenntniss vermittelte von der eigentlichen Natur der Zahl π, zugleich eins der berühmtesten Probleme der Mathematik endgiltig, wenn auch in negativem Sinne, erledigt zu haben; und dies Verdienst wird auf keine Weise durch die grössere Einfachheit geschmälert, welche dem späteren Beweise von Weierstrass vor dem seinigen den Vorzug giebt. Aber freilich darf man nicht vergessen, wie ihm durch die geistvolle Untersuchung des Herrn Ch. Hermite über die Zahl e die principielle Grundlage schon gegeben war, auf der er nur weiterzubauen brauchte und die allein den Erfolg seiner Bemühungen ermöglichte.

7. Die Abhandlung von Weierstrass enthält nun auch noch den Beweis einiger allgemeineren Sätze, welche Lindemann gleichfalls schon ausgesprochen, aber ohne ausgeführten Beweis gelassen hat. Wir wollen uns, indem wir in dieser Hinsicht auf die Abhandlung selbst verweisen, damit begnügen, nur diese Sätze selbst hier anzufügen.

Sind $x_1, x_2, \ldots x_r$ die als verschieden vorausgesetzten Wurzeln einer Gleichung

$$x^r + C_1 x^{r-1} + \cdots + C_r = 0$$

mit rationalen Coefficienten, $X_1, X_2, \ldots X_r$ aber ganze (oder auch nur rationale) Zahlen, unter denen wenigstens eine nicht Null ist, so ist die Gleichheit

$$\sum_{i=1}^{r} X_i e^{x_i} = 0$$

unmöglich. Dieser Satz enthält in sich die von Hermite bezüglich der Zahl e gewonnene Erkenntniss; denn er besagt, wenn man für $x_1, x_2, \ldots x_r$ irgend r von einander verschiedene ganze Zahlen wählt, dass e keine algebraische Zahl sein kann. Er lässt zudem leicht eine Verallgemeinerung zu, indem man unter $x_1, x_2, \ldots x_r$ irgend r von einander verschiedene algebraische Zahlen verstehen darf.

Endlich aber lässt der Satz noch eine Erweiterung zu und verwandelt sich so in den nachstehenden, welcher alle die vorigen umfasst:

Allgemeinster Satz: Bedeuten $x_1, x_2, \ldots x_r$ irgend r von einander *verschiedene*, $X_1, X_2, \ldots X_r$ aber *beliebige* algebraische Zahlen, von deren letztern eine wenigstens von Null verschieden ist, so ist die Gleichung

$$\sum_{i=1}^{r} X_i e^{x_i} = 0 \tag{21}$$

unmöglich.

Wählt man z. B. $r = 2$, $X_1 = -1$, $x_2 = 0$ und ersetzt x_1, X_2 durch die Zeichen x, X, so nimmt vorstehende Gleichung die Form an

$$e^x = X. \tag{22}$$

Dem allgemeinen Satze gemäss kann diese nicht bestehen, wenn x, X gleichzeitig algebraische Zahlen und x von $x_2 = 0$ verschieden ist. Demnach findet der besondere Satz statt:

Die Exponentialgrösse e^x ist stets eine transcendente Zahl, wenn x eine von Null verschiedene algebraische Zahl ist.

Da x in der Gleichung (22) der natürliche Logarithmus von X ist und dem Werthe $x = 0$ der Werth $X = 1$ entsprechen würde, folgt aus (21) gleichermassen auch folgender zugehörige zweite Satz:

Der natürliche Logarithmus einer algebraischen Zahl X ist immer eine transcendente Zahl, wenn X nicht den Werth 1 hat.

Zehnte Vorlesung.

Ueber die kubischen Irrationellen.

1. Während wir in den voraufgehenden Vorlesungen von Untersuchungen berichten konnten, welche ihren endgiltigen Abschluss bereits gefunden haben, wollen wir nun zum Schlusse noch eine Frage berühren, die noch vieler eingehender Untersuchungen bedürfen wird, bevor sie in einer ähnlich befriedigenden Weise beantwortet sein wird. In der vierten Vorlesung haben wir für die quadratischen Irrationellen ein ihnen durchaus eigenthümliches arithmetisches Kennzeichen hergeleitet, darin bestehend, dass sie und nur sie allein in einen periodischen Kettenbruch der dort näher angegebenen Art entwickelt werden können. Es ist auch bereits daran die Frage geknüpft worden, ob für die Irrationellen höheren Grades ein ähnliches arithmetisches Kennzeichen vorhanden sei und worin es bestehe.

Wie wichtig und interessant der Nachweis eines solchen sein würde und welch reiches Feld der Forschung sich hier eröffnet, ist kaum nöthig besonders hervorzuheben; es sei aber erlaubt, eine Stelle aus Hermite's zahlentheoretischen, an Jacobi gerichteten Briefen*) ausführlich hier beizubringen, welche sehr anregend über diese Frage sich äussert. Sie findet

*) Extrait de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres.

sich in Crelle's Journal Bd. 40 pag. 286 und lautet folgendermassen: Mais permettez-moi, Monsieur, de revenir un instant sur les circonstances remarquables, auxquelles donne lieu la réduction des formes dont les coefficiens dépendent de racines d'équations algébriques à coefficiens entiers. Peut-être parviendra-t-on à déduire de là un système complet de caractères pour chaque espèce de ce genre de quantités, analogue par exemple à ceux que donne la théorie des fractions continues pour les racines des équations du second degré. On ne peut du moins faire concourir trop d'éléments pour jeter quelque lumière sur cette variété infinie des irrationnelles algébriques, dont les symboles d'extraction de racines ne nous représentent que la plus faible partie. Ici comme dans la théorie des transcendentes il a été facile de trouver à une longue suite de notions analytiques de plus en plus complexes une origine commune, une définition unique et complète, où n'entrent que les premiers éléments du calcul; mais quelle tâche immense, pour la théorie des nombres et le calcul intégral, de pénétrer dans la nature d'une telle multiplicité d'êtres de raison, en les classant en groupes irréductibles entre eux, de les constituer tous individuellement par des définitions caractéristiques et élémentaires?

Wie man sieht, giebt Hermite in dieser Stelle auch einen Fingerzeig, auf welcher Grundlage etwa die Lösung der Aufgabe zu suchen sei, nämlich vermittelst der „Reduktion der sogenannten zahlentheoretischen Formen". In der That, nachdem durch Lagrange, wie wir in der vierten Vorlesung gesehen, der innige Zusammenhang der Frage bezüglich der quadratischen Irrationellen mit der Theorie der quadratischen Formen aufgedeckt worden ist, lag die Vermuthung sehr nahe, dass zwischen dem Verhalten höherer Irrationellen und der Theorie der höheren Formen eine analoge Beziehung bestehe. Und Hermite hat aus dieser Erwägung eine Reihe von Untersuchungen begonnen und in seinen Briefen auseinandergesetzt, welche hauptsächlich zunächst dahin zielen, geeignete Definitionen der „reducirten Formen" höherer Art zu liefern und nachzuweisen, dass bei der Berechnung derselben aus einer ursprünglich gegebenen Form eine gewisse Periodicität sich herausstellen müsse. Einer seiner Schüler, Herr

Charve*), hat in einer ausführlichen Arbeit über ternäre quadratische Formen, welcher er diejenige Auffassung reducirter Formen zu Grunde legt, die man Selling**) verdankt, die Hermite'schen Gedanken entwickelt und bestätigt, indem er die arithmetische Operation der Reduktion einer Form zugleich geometrisch veranschaulicht; theils theoretisch, theils an einer Reihe numerischer Beispiele findet er eine Periodicität in der Reihe der Substitutionen, welche die reducirten Formen aus der ursprünglich gegebenen Form herzuleiten geeignet sind.

Andererseits hat Jacobi auf dem vorliegenden unerforschten Gebiete einen wichtigen Schritt voran gethan, der gewiss die richtige Fährte verfolgt. In einer Abhandlung, welche erst nach seinem Tode veröffentlicht worden ist***), entwickelt er einen Algorithmus, der als eine sehr nahe liegende Verallgemeinerung desjenigen anzusehen ist, auf welchen wir in der 3. und 4. Vorlesung die Kettenbrüche und ihre Periodicität im Falle der quadratischen Irrationellen begründet haben und welchen er deshalb auch einen Kettenbruchalgorithmus nennt; und indem er denselben zur Anwendung bringt auf die Kubikwurzel aus einer ganzen Zahl, findet er an verschiedenen numerischen Beispielen die Vermuthung bestätigt, dass der Algorithmus periodisch sei. Die sehr interessante Frage, ob diese Eigenschaft der Kubikwurzel allgemein und derselben bez. den Irrationellen dritten Grades charakteristisch sei, blieb leider einstweilen ungelöst; denn, obwohl sie nach den Ergebnissen von Hermite und Charve unzweifelhaft bejahend zu beantworten sein dürfte, können doch die genannten Untersuchungen nicht als entscheidend dafür gelten, solange zwischen ihnen und dem Kettenbruchalgorithmus nicht ein fester Zusammenhang nachgewiesen worden ist.

*) Thèses prés. à la faculté des Sciences de Paris: de la réduction des formes quadratiques ternaires positives et de leur application aux irrationnelles du troisième degré.

**) Journal f. d. r. u. a. M. Bd. 77.

***) Jacobi, allgem. Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus drei vorhergehenden gebildet wird; herausg. von Heine, Journ. f. d. r. u. a. Math. Bd. 69 pag. 29.

Auch eine Arbeit von Fürstenau (über Kettenbrüche höherer Ordnung, im Jahresberichte über das Königl. Realgymnasium zu Wiesbaden 1874) giebt diese Lösung nicht. Ihm gebührt zwar das Verdienst, analytische Ausdrücke, die sogenannten Kettenbrüche höherer, insbesondere zweiter Ordnung aufgefunden zu haben, welche den Jacobi'schen Algorithmen genau so entsprechen, wie dem von uns in der 3. Vorlesung zu Grunde gelegten Algorithmus die gewöhnlichen Kettenbrüche; ob er so zugleich an Stelle jenes Kettenbruchalgorithmus etwas Uebersichtlicheres gesetzt hat, das vor ihm den Vorzug verdiene, muss ich in Frage stellen; mir wenigstens scheint den Rekursionsformeln von Jacobi, aus denen aufs Einfachste alle Folgerungen sich herleiten, vor den sehr weitschichtigen Ausdrücken von Fürstenau der Vorrang zuzukommen. Jedenfalls gelingt es Fürstenau nur, den nicht schwierigen Nachweis zu führen, dass, wenn der Kettenbruch zweiter Ordnung, welcher einer Grösse x gleich ist, ein periodischer ist, x Wurzel einer kubischen Gleichung mit ganzzahligen Coefficienten sein muss; die Umkehrung aber, welche eigentlich das Wesentlichere der Frage ist, bleibt gänzlich unerörtert. Wir wollen im Folgenden das Ergebniss von Fürstenau bestätigen, indem wir aber formell an dem Kettenbruchalgorithmus von Jacobi selbst festhalten.

Ausserdem aber hat der Verfasser dieses Buches den Versuch gemacht*), jene Umkehrung, d. i. die von Jacobi an einzelnen Beispielen bemerkte Thatsache als allgemein giltig zu beweisen. Er glaubte dies Ziel dadurch erreichen zu können, dass er die in der vierten Vorlesung dargestellte Untersuchung von Lagrange in ganz analoger Weise auf den hier vorliegenden Fall, nämlich auf gewisse ternäre kubische Formen übertrug. Wenn ihm freilich bisher der gesuchte Nachweis so noch nicht gelungen ist, so dürften doch, bis Vollkommeneres gewonnen worden ist, die Ergebnisse dieser Untersuchung des Interesses namentlich deshalb nicht entbehren, weil sie aufs deutlichste zeigen, dass die Jacobi'schen Algorithmen mit den obgenannten Hermite'schen Gesichts-

*) Journ. f. d. r. u. a. Math. Bd. 75, pag. 25.

punkten in der That in Verbindung sein müssen; und so sollen sie als einstweiliger Abschluss der Untersuchungen über die Natur der algebraischen Irrationellen zum Schlusse noch dargestellt werden.

2. Um zunächst den Jacobi'schen Kettenbruchalgorithmus seinem Wesen nach zu bezeichnen, führen wir drei Unbestimmte a_0, a_1, a_2 ein und leiten aus ihnen durch die Beziehungen:

$$(1)\qquad \begin{cases} a_0 + l_0 a_1 + m_0 a_2 = a_3 \\ a_1 + l_1 a_2 + m_1 a_3 = a_4 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_i + l_i a_{i+1} + m_i a_{i+2} = a_{i+3}, \end{cases}$$

in welchen

$$(2)\qquad l_0, l_1, l_2, \ldots, \quad m_0, m_1, m_2, \ldots$$

beliebig gegebene Grössen bedeuten, andere Grössen a_3, a_4, ... in beliebiger Menge her. Vermittelst dieser Beziehungen ist schon a_3 durch a_0, a_1, a_2 linear ausgedrückt; wird sein Werth in die zweite Gleichung eingesetzt, so wird es auch a_4, und wenn a_3 und a_4 in die folgende Gleichung eingesetzt werden, auch a_5 u. s. w., sodass man schliesslich drei Gleichungen folgender Gestalt erhalten wird:

$$(3)\qquad \begin{cases} a_i = P_i a_0 + P'_i a_1 + P''_i a_2 \\ a_{i+1} = P_{i+1} a_0 + P'_{i+1} a_1 + P''_{i+1} a_2 \\ a_{i+2} = P_{i+2} a_0 + P'_{i+2} a_1 + P''_{i+2} a_2; \end{cases}$$

die Coefficienten P, P', P'' werden dabei sämmtlich positive ganze Zahlen sein, wenn wir dies, wie es von vornherein geschehen soll, von den Zahlen (2) voraussetzen; denn sie entstehen dann aus diesen positiven ganzen Zahlen, indem mit denselben nur Additionen und Multiplikationen zur Ausführung gebracht werden. In diesen Gleichungen ist der Sache nach $i > 3$ vorausgesetzt, d. h. sie geben die Werthe der Zahlen a_3, a_4, a_5, ...; jedoch liefern sie offenbar auch die Zahlen a_0, a_1, a_2, gelten also für jeden Index i, wenn folgende Werthe festgesetzt werden:

$$(4) \quad \begin{cases} P_0 = 1, & P_0' = 0, & P_0'' = 0 \\ P_1 = 0, & P_1' = 1, & P_1'' = 0 \\ P_2 = 0, & P_2' = 0, & P_2'' = 1. \end{cases}$$

So liefert dann die letzte der Gleichungen (3), wenn i in $i+1$ verwandelt wird, für jeden Werth des Index i die folgende:

$$a_{i+3} = P_{i+3}a_0 + P'_{i+3}a_1 + P''_{i+3}a_2;$$

andererseits findet man, wenn in die letzte der Gleichungen (1) die Werthe (3) eingesetzt werden,

$$\begin{aligned} a_{i+3} = {} & (P_i + l_i P_{i+1} + m_i P_{i+2})a_0 \\ & + (P_i' + l_i P'_{i+1} + m_i P'_{i+2})a_1 \\ & + (P_i'' + l_i P''_{i+1} + m_i P''_{i+2})a_2. \end{aligned}$$

Dieser Werth muss also dem vorigen gleich sein und ergiebt wegen der Unbestimmtheit der Grössen a_0, a_1, a_2 folgende drei Beziehungen zwischen den aufeinanderfolgenden P_i, P_i', P_i'':

$$(5) \quad \begin{cases} P_i + l_i P_{i+1} + m_i P_{i+2} = P_{i+3} \\ P_i' + l_i P'_{i+1} + m_i P'_{i+2} = P'_{i+3} \\ P_i'' + l_i P''_{i+1} + m_i P''_{i+2} = P''_{i+3}. \end{cases}$$

Wird demnach die Determinante der Gleichungen (3) mit Π bezeichnet,

$$\Pi = \begin{vmatrix} P_i, & P_i', & P_i'' \\ P_{i+1}, & P'_{i+1}, & P''_{i+1} \\ P_{i+2}, & P'_{i+2}, & P''_{i+2} \end{vmatrix},$$

so lässt sich mit Rücksicht auf die vorstehenden Beziehungen nach bekannten einfachen Determinantensätzen dieselbe auch so schreiben:

$$\Pi = \begin{vmatrix} P_{i+1}, & P'_{i+1}, & P''_{i+1} \\ P_{i+2}, & P'_{i+2}, & P''_{i+2} \\ P_{i+3}, & P'_{i+3}, & P''_{i+3} \end{vmatrix},$$

d. h. sie ändert sich nicht, wenn der Index i um eine Einheit vermehrt oder vermindert wird, und ist demnach schliesslich gleich der Determinante

$$\begin{vmatrix} P_0, & P_0', & P_0'' \\ P_1, & P_1', & P_1'' \\ P_2, & P_2', & P_2'' \end{vmatrix},$$

welche den unter (4) festgesetzten Werthen ihrer Elemente zufolge gleich 1 ist. Man hat also die Gleichung:

$$(6) \qquad \begin{vmatrix} P_i, & P_i', & P_i'' \\ P_{i+1}, & P_{i+1}', & P_{i+1}'' \\ P_{i+2}, & P_{i+2}', & P_{i+2}'' \end{vmatrix} = 1.$$

Hieraus folgt weiter, dass durch Auflösung der Gleichungen (3) nach a_0, a_1, a_2 für jedes i drei Gleichungen hervorgehen von folgender Gestalt:

$$(7) \qquad \left\{ \begin{aligned} a_0 &= p_i a_i + q_i a_{i+1} + r_i a_{i+2} \\ a_1 &= p_i' a_i + q_i' a_{i+1} + r_i' a_{i+2} \\ a_2 &= p_i'' a_i + q_i'' a_{i+1} + r_i'' a_{i+2}, \end{aligned} \right.$$

deren Coefficienten ganze Zahlen sind. Die Determinante dieser aufgelösten Gleichungen ist aber bekanntlich dem reciproken Werthe der Determinante der ursprünglichen Gleichungen (3) gleich, und folglich findet sich die fernere Gleichung:

$$(8) \qquad \begin{vmatrix} p_i, & q_i, & r_i \\ p_i', & q_i', & r_i' \\ p_i'', & q_i'', & r_i'' \end{vmatrix} = 1,$$

und die einzelnen Elemente der Determinante (6) werden die zu den entsprechenden Elementen der Determinante (8) adjungirten zweigliedrigen Unterdeterminanten sein, und umgekehrt.

Wird endlich in der ersten der Gleichungen (7) i in $i+1$ verwandelt, sodass

$$a_0 = p_{i+1} a_{i+1} + q_{i+1} a_{i+2} + r_{i+1} a_{i+3}$$

erhalten wird, und nun statt a_{i+3} sein Werth nach den Gleichungen (1) eingesetzt, so kommt

$$a_0 = r_{i+1} a_i + (p_{i+1} + l_i r_{i+1}) a_{i+1} + (q_{i+1} + m_i r_{i+1}) a_{i+2},$$

eine Gleichung, welche mit der ersten der Gleichungen (7) verglichen, und wenn man bedenkt, dass in den Beziehungen (1)

ebenso gut wie a_0, a_1, a_2 auch die letzten drei Grössen a_{i+1}, a_{i+2}, a_{i+3} als die beliebigen, gegebenen Grössen aufgefasst werden können, aus denen dann die übrigen vermittelst jener Beziehungen hervorgehen, noch folgende Gleichungen erschliessen lässt:

$$(9)\quad r_{i+1} = p_i,\quad p_{i+1} + l_i r_{i+1} = q_i,\quad q_{i+1} + m_i r_{i+1} = r_i$$

oder umgekehrt:

$$(10)\quad p_{i+1} = q_i - l_i p_i,\quad q_{i+1} = r_i - m_i p_i,\quad r_{i+1} = p_i.$$

Diese Gleichungen können dazu dienen, die Coefficienten der Gleichungen (7) allmählich zu berechnen ohne Zwischenkunft der Grössen P_i, P_i', P_i''. Da die mittlere der Formeln (9), wenn i in $i+1$ verwandelt wird,

$$q_{i+1} = p_{i+2} + l_{i+1} r_{i+2}\quad \text{d. h.}\quad p_{i+2} + l_{i+1} p_{i+1},$$

und die mittlere der Gleichungen (10) für $i > 0$

$$q_{i+1} = p_{i-1} - m_i p_i$$

ergiebt, so erhält man durch Vergleichung beider Ausdrücke noch die Beziehung

$$(11)\qquad p_{i+2} = p_{i-1} - m_i p_i - l_{i+1} p_{i+1},$$

um die Grössen p_i aus den jedesmal vorhergehenden drei ähnlichen Grössen zu berechnen, worauf dann die Formeln (10) die Grössen q_i und r_i finden lassen.

Ganz die gleichen Beziehungen, welche die Formeln (9), (10) und (11) zwischen den Grössen p_i, q_i, r_i ausdrücken, bestehen aber offenbar auch zwischen den Grössen p_i', q_i', r_i' bez. zwischen den Grössen p_i'', q_i'', r_i''.

3. Wir wollen nunmehr die bisher beliebigen positiven ganzen Zahlen l_i, m_i bestimmter wählen. Unter u_0, v_0, w_0 nämlich wollen wir drei gegebene positive Werthe verstehen, von welchen w_0 der grösste sei. Dann seien l_0, m_0 die den Brüchen $\frac{v_0}{u_0}$, $\frac{w_0}{u_0}$ nächst kleineren ganzen Zahlen; indem man setzt

$$v_0 - l_0 u_0 = u_1,\quad w_0 - m_0 u_0 = v_1,\quad u_0 = w_1,$$

seien l_1, m_1 die den Brüchen $\frac{v_1}{u_1}$, $\frac{w_1}{u_1}$ nächst kleineren Ganzen, dann

$$v_1 - l_1 u_1 = u_2, \quad w_1 - m_1 u_1 = v_2, \quad u_1 = w_2,$$

wiederum l_2, m_2 die den Brüchen $\frac{v_2}{u_2}$, $\frac{w_2}{u_2}$ nächst kleineren Ganzen u. s. f., sodass allgemein l_i, m_i die den Brüchen $\frac{v_i}{u_i}$, $\frac{w_i}{u_i}$ nächst kleineren Ganzen sind und aus u_i, v_i, w_i die nächstfolgenden u_{i+1}, v_{i+1}, w_{i+1} durch die Formeln

$$(12) \qquad v_i - l_i u_i = u_{i+1}, \quad w_i - m_i u_i = v_{i+1}, \quad u_i = w_{i+1}$$

gewonnen werden. Bedeuten jetzt in den rekurrirenden Gleichungen (1) l_i, m_i die so bestimmten positiven ganzen Zahlen, so werden alle Resultate der vorigen Nummer Bestand behalten. Wir wollen den Algorithmus (1) dann den zu den Werthen $\frac{v_0}{u_0}$, $\frac{w_0}{u_0}$ gehörigen Kettenbruchalgorithmus nennen.

Setzt man nun

$$(13) \qquad U = a_0 u_0 + a_1 v_0 + a_2 w_0$$

und

$$(14) \qquad U_i = a_i u_i + a_{i+1} v_i + a_{i+2} w_i,$$

so ist leicht ersichtlich, dass der letztere Ausdruck unverändert bleibt, wenn i in $i+1$ verwandelt wird, und dass demnach die Ausdrücke (13), (14) einander gleich sind. Denn ersetzt man in

$$U_{i+1} = a_{i+1} u_{i+1} + a_{i+2} v_{i+1} + a_{i+3} w_{i+1}$$

die Grössen u_{i+1}, v_{i+1}, w_{i+1} durch ihre Werthe (12), so wird

$$U_{i+1} = a_{i+1} v_i + a_{i+2} w_i + (a_{i+3} - m_i a_{i+2} - l_i a_{i+1}) u_i$$

d. h. der letzten der Gleichungen (1) zufolge

$$U_{i+1} = a_i u_i + a_{i+1} v_i + a_{i+2} w_i = U_i.$$

Hiernach besteht die Gleichung

$$a_i u_i + a_{i+1} v_i + a_{i+2} w_i = a_0 u_0 + a_1 v_0 + a_2 w_0.$$

Werden nun hierin für a_i, a_{i+1}, a_{i+2} ihre Werthe (3) eingesetzt und die Coefficienten der Unbestimmten a_0, a_1, a_2 auf beiden Seiten mit einander verglichen, so gehen daraus folgende drei Beziehungen hervor:

$$(15)\quad \begin{cases} u_0 = P_i u_i + P_{i+1} v_i + P_{i+2} w_i \\ v_0 = P'_i u_i + P'_{i+1} v_i + P'_{i+2} w_i \\ w_0 = P''_i u_i + P''_{i+1} v_i + P''_{i+2} w_i, \end{cases}$$

aus denen, wie die Gleichungen (7) aus den Gleichungen (5), durch Umkehrung noch die nachstehenden erschlossen werden können:

$$(16)\quad \begin{cases} u_i = p_i u_0 + p'_i v_0 + p''_i w_0 \\ v_i = q_i u_0 + q'_i v_0 + q''_i w_0 \\ w_i = r_i u_0 + r'_i v_0 + r''_i w_0 . \end{cases}$$

Setzen wir jetzt den Fall, in der Reihe der Systeme $\frac{v_i}{u_i}, \frac{w_i}{u_i}$, welche den aufeinanderfolgenden Werthen des Index i entsprechen, kehre einmal eins wieder, sodass etwa

$$(17)\quad \frac{v_{k+h}}{u_{k+h}} = \frac{v_k}{u_k}, \quad \frac{w_{k+h}}{u_{k+h}} = \frac{w_k}{u_k}$$

sei. Dann werden natürlich auch die diesen Brüchen nächst kleineren Ganzen übereinstimmen, d. h.

$$l_{k+h} = l_k, \quad m_{k+h} = m_k$$

sein. Aus (12) folgen die Gleichungen

$$\frac{v_{k+1}}{u_{k+1}} = \frac{\frac{w_k}{u_k} - m_k}{\frac{v_k}{u_k} - l_k}, \quad \frac{w_{k+1}}{u_{k+1}} = \frac{1}{\frac{v_k}{u_k} - l_k};$$

sie lehren offenbar, dass unter den gemachten Voraussetzungen auch $\frac{v_{k+1}}{u_{k+1}}, \frac{w_{k+1}}{u_{k+1}}$ sich nicht ändern, wenn der Index um h Einheiten wächst, dass mit andern Worten auch

$$\frac{v_{k+h+1}}{u_{k+h+1}} = \frac{v_{k+1}}{u_{k+1}}, \quad \frac{w_{k+h+1}}{u_{k+h+1}} = \frac{w_{k+1}}{u_{k+1}}$$

und folglich auch

$$l_{k+h+1} = l_{k+1}, \quad m_{k+h+1} = m_{k+1}$$

ist. So kann man gleicherweise fortschreiten und findet also allmählich auch

$$\frac{v_{k+2h}}{u_{k+2h}} = \frac{v_{k+h}}{u_{k+h}}, \quad \frac{w_{k+2h}}{u_{k+2h}} = \frac{w_{k+h}}{u_{k+h}},$$

d. h. mit Rücksicht auf die ursprüngliche Annahme

$$\frac{v_{k+2h}}{u_{k+2h}} = \frac{v_k}{u_k}, \quad \frac{w_{k+2h}}{u_{k+2h}} = \frac{w_k}{u_k}. \tag{18}$$

Die beiden ersten der Gleichungen (15) aber liefern für das Verhältniss $\frac{v_0}{u_0}$ folgenden Werth:

$$\frac{v_0}{u_0} = \frac{P'_i + P'_{i+1} \cdot \frac{v_i}{u_i} + P'_{i+2} \cdot \frac{w_i}{u_i}}{P_i + P_{i+1} \cdot \frac{v_i}{u_i} + P_{i+2} \cdot \frac{w_i}{u_i}},$$

oder die Gleichung

$$0 = \left(P_i \cdot \frac{v_0}{u_0} - P'_i\right) + \frac{v_i}{u_i}\left(P_{i+1} \cdot \frac{v_0}{u_0} - P'_{i+1}\right) \\ + \frac{w_i}{u_i}\left(P_{i+2} \cdot \frac{v_0}{u_0} - P'_{i+2}\right).$$

Indem wir in der letztern für i die drei Werthe k, $k+h$, $k+2h$ einsetzen und die Gleichungen (17) und (18) beachten, gewinnen wir folgende drei Gleichungen:

$$0 = P_k \cdot \frac{v_0}{u_0} - P'_k + \frac{v_k}{u_k}\left(P_{k+1} \cdot \frac{v_0}{u_0} - P'_{k+1}\right) \\ + \frac{w_k}{u_k}\left(P_{k+2} \cdot \frac{v_0}{u_0} - P'_{k+2}\right)$$

$$0 = P_{k+h} \cdot \frac{v_0}{u_0} - P'_{k+h} + \frac{v_k}{u_k}\left(P_{k+h+1} \cdot \frac{v_0}{u_0} - P'_{k+h+1}\right) \\ + \frac{w_k}{u_k}\left(P_{k+h+2} \cdot \frac{v_0}{u_0} - P'_{k+h+2}\right)$$

$$0 = P_{k+2h} \cdot \frac{v_0}{u_0} - P'_{k+2h} + \frac{v_k}{u_k}\left(P_{k+2h+1} \cdot \frac{v_0}{u_0} - P'_{k+2h+1}\right) \\ + \frac{w_k}{u_k}\left(P_{k+2h+2} \cdot \frac{v_0}{u_0} - P'_{k+2h+2}\right),$$

welche nur bestehen können, wenn ihre Determinante verschwindet. So ergiebt sich die Bedingung:

$$0 = \begin{vmatrix} P_k \cdot \frac{v_0}{u_0} - P'_k, & P_{k+1} \cdot \frac{v_0}{u_0} - P'_{k+1}, & P_{k+2} \cdot \frac{v_0}{u_0} - P'_{k+2} \\ P_{k+h} \cdot \frac{v_0}{u_0} - P'_{k+h}, & P_{k+h+1} \cdot \frac{v_0}{u_0} - P'_{k+h+1}, & P_{k+h+2} \cdot \frac{v_0}{u_0} - P'_{k+h+2} \\ P_{k+2h} \cdot \frac{v_0}{u_0} - P'_{k+2h}, & P_{k+2h+1} \cdot \frac{v_0}{u_0} - P'_{k+2h+1}, & P_{k+2h+2} \cdot \frac{v_0}{u_0} - P'_{k+2h+2} \end{vmatrix}.$$

Sie ist, entwickelt gedacht, in Bezug auf $\frac{v_0}{u_0}$ eine kubische Gleichung, deren sämmtliche Coefficienten ganze Zahlen sind. Denn diese setzen sich aus den ganzzahligen P_i, P'_i, P''_i durch Additionen, Subtraktionen und Multiplikationen zusammen. Ganz dasselbe Ergebniss kann aus der ersten und dritten der Gleichungen (15) bezüglich des Verhältnisses $\frac{w_0}{u_0}$ hergeleitet werden, und so finden wir endlich den Satz, welcher mit dem von Fürstenau im Wesentlichen identisch ist: Ist der zu den Grössen $\frac{v_0}{u_0}$, $\frac{w_0}{u_0}$ gehörige Kettenbruchalgorithmus periodisch, d. h. stösst man bei ihm auf die Gleichungen (17), so sind $\frac{v_0}{u_0}$, $\frac{w_0}{u_0}$ gleichzeitig Wurzeln kubischer Gleichungen mit ganzzahligen Coefficienten, d. h. sie sind kubische Irrationellen.

4. Wir wenden uns nunmehr zu der umgekehrten Frage, ob für alle kubischen Irrationellen der Jacobi'sche Kettenbruchalgorithmus periodisch sei oder nicht; wir werden uns bei ihrer Behandlung auf den einfachsten Fall beschränken, in welchem die Irrationelle eine Kubikwurzel aus einer ganzen Zahl ist, beginnen aber mit einigen allgemeiner giltigen Bemerkungen.

Die kubische Gleichung, welcher die Irrationelle genügt, sei die Gleichung

$$(19) \qquad x^3 + c_1 x^2 + c_2 x + c_3 = 0$$

mit ganzzahligen Coefficienten, und von ihren Wurzeln α, β, γ sei die eine, etwa α, reell und positiv, die beiden andern β, γ conjugirt imaginär. Unter einer ganzen complexen Zahl verstehen wir jeden Ausdruck von der Form

$$r\alpha^2 + s\alpha + t$$

mit ganzzahligen Coefficienten r, s, t, und nennen jeden gemeinsamen Theiler dieser Coefficienten einen Theiler der complexen Zahl. Die Ausdrücke, welche aus jenem hervorgehen, wenn α durch β und γ ersetzt wird, und welche offenbar zu einander conjugirt imaginär sind, heissen die ihm conjugirten complexen Zahlen. Das Produkt aller drei conjugirt complexen Zahlen, nämlich

$$(r\alpha^2 + s\alpha + t)(r\beta^2 + s\beta + t)(r\gamma^2 + s\gamma + t)$$

heisst ihre gemeinsame Norm.

Hier gelten zunächst folgende einfache Bemerkungen:

1) Sind

$$r\alpha^2 + s\alpha + t, \quad r'\alpha^2 + s'\alpha + t'$$

zwei ganze complexe Zahlen, so lässt sich dem Produkte

$$(r\alpha^2 + s\alpha + t)(r'\alpha^2 + s'\alpha + t')$$

vermittelst der Identität

$$\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0$$

wieder die Gestalt einer ganzen complexen Zahl

$$r''\alpha^2 + s''\alpha + t''$$

geben.

2) Da β, γ die Wurzeln der Gleichung

$$x^2 + (\alpha + c_1)x + \alpha^2 + c_1\alpha + c_2 = 0$$

also

$$\beta + \gamma = -(\alpha + c_1), \quad \beta\gamma = \alpha^2 + c_1\alpha + c_2$$

sind, findet sich leicht, dass das Produkt

$$(r\beta^2 + s\beta + t)\cdot(r\gamma^2 + s\gamma + t),$$

dessen Werth positiv ist, da die Faktoren conjugirt imaginär sind, als eine ganze complexe Zahl

$$r_1\alpha^2 + s_1\alpha + t_1$$

geschrieben werden kann.

3) Die Norm einer complexen ganzen Zahl:

$$(r\alpha^2 + s\alpha + t) \cdot (r\beta^2 + s\beta + t) \cdot (r\gamma^2 + s\gamma + t)$$

ist, als ganze und ganzzahlige symmetrische Funktion von den Wurzeln der Gleichung (19), gleich einer reellen ganzen Zahl.

Dies vorausgeschickt, verstehen wir unter den Zeichen u_0, v_0, w_0 jetzt die Werthe

$$u_0 = 1, \quad v_0 = \alpha, \quad w_0 = \alpha^2$$

und bilden den Jacobi'schen Kettenbruchalgorithmus, welcher zu den Grössen $\frac{v_0}{u_0} = \alpha$, $\frac{w_0}{u_0} = \alpha^2$ gehört, jedoch auf folgende, von der früheren etwas abweichende Weise: Wir nennen l_0, m_0 die grössten Ganzen, welche in

$$\frac{v_0}{u_0} = \alpha, \quad \frac{w_0}{u_0} = \alpha^2$$

enthalten sind, der Art, dass

$$v_0 - l_0 u_0, \quad w_0 - m_0 u_0$$

positive Werthe bezeichnen. Aus den Grössen

$$u_0, v_0, w_0, l_0, m_0$$

bilden wir nun andere:

$$u_1, v_1, w_1, l_1, m_1,$$

aus diesen wieder andere:

$$u_2, v_2, w_2, l_2, m_2$$

u. s. w. nach bestimmtem Gesetze. Wir bezeichnen nämlich mit l_i, m_i jedesmal die in den Brüchen $\frac{v_i}{u_i}$, $\frac{w_i}{u_i}$ enthaltenen nächst kleineren ganzen Zahlen, sodass immer

$$v_i - l_i u_i, \quad w_i - m_i u_i, \quad u_i$$

positive Werthe werden, sobald es die Grössen u_i, v_i, w_i schon sind. Ist ferner schon u_i eine ganze Zahl, und v_i, w_i complexe ganze Zahlen, so sind letzteres auch $v_i - l_i u_i$, $w_i - m_i u_i$. Werden daher unter v_i', v_i'' die zu v_i conjugirten Zahlen verstanden, so ist nach 2) der positive Ausdruck

$$f_i = (v_i' - l_i u_i)(v_i'' - l_i u_i) \tag{20}$$

eine complexe ganze Zahl, und die drei Produkte

$$(21)\qquad f_i(v_i - l_i u_i),\quad f_i(w_i - m_i u_i),\quad f_i u_i$$

nach 1) ebenfalls complexe ganze Zahlen, das erste sogar nach 3) eine reelle ganze Zahl, alle drei von positivem Werthe. Nennt man endlich g_i die grösste, positiv genommene ganze Zahl, die gleichzeitig Theiler aller drei Zahlen (21) ist, so sollen aus den vorhergehenden Grössen

$$u_i,\ v_i,\ w_i$$

die jedesmal folgenden u_{i+1}, v_{i+1}, w_{i+1} durch nachstehende Gleichungen gebildet werden:

$$(22)\qquad \begin{cases} g_i u_{i+1} = f_i(v_i - l_i u_i) \\ g_i v_{i+1} = f_i(w_i - m_i u_i) \\ g_i w_{i+1} = f_i u_i . \end{cases}$$

Da für $i = 0$ die bezüglich u_i, v_i, w_i gemachten Voraussetzungen erfüllt sind, so bleiben u_i, v_i, w_i hiernach für jeden Werth des Index i positive Werthe, die erste eine reelle, die beiden andern complexe ganze Zahlen, während l_i, m_i stets positive ganze Zahlen oder die Null bedeuten. Wird noch

$$(23)\qquad F_0 = 1$$

und für $i > 0$

$$(24)\qquad F_i = \frac{f_0}{g_0} \cdot \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} \cdots \frac{f_{i-1}}{g_{i-1}}$$

gesetzt, so nehmen die Gleichungen (22) die Gestalt an:

$$(25)\qquad \begin{cases} \dfrac{u_{i+1}}{F_{i+1}} = \dfrac{v_i}{F_i} - l_i \cdot \dfrac{u_i}{F_i} \\[2ex] \dfrac{v_{i+1}}{F_{i+1}} = \dfrac{w_i}{F_i} - m_i \cdot \dfrac{u_i}{F_i} \\[2ex] \dfrac{w_{i+1}}{F_{i+1}} = \dfrac{u_i}{F_i} . \end{cases}$$

Die Vergleichung dieser Beziehungen mit den Gleichungen (12), sowie die Bemerkung, dass die Grössen $\dfrac{u_i}{F_i}$, $\dfrac{v_i}{F_i}$, $\dfrac{w_i}{F_i}$ dieselben Verhältnisse haben wie bez. die Grössen u_i, v_i, w_i zu einander, lässt erkennen, dass gegenwärtig die Grössen

$$\frac{u_i}{F_i},\ \frac{v_i}{F_i},\ \frac{w_i}{F_i},\ l_i,\ m_i$$

genau in derselben Weise zu einander bestimmt sind, wie früher die Grössen

$$u_i,\ v_i,\ w_i,\ l,\ m:$$

infolge davon müssen zwischen jenen dieselben Formeln bestehen, die wir in voriger Nummer für die letztern hergeleitet haben; z. B. finden sich an Stelle der Gleichungen (15) und (16) gegenwärtig nachstehende Gleichungen:

$$(26)\quad \begin{cases} F_i u_0 = P_i u_i + P_{i+1} v_i + P_{i+2} w_i \\ F_i v_0 = P'_i u_i + P'_{i+1} v_i + P'_{i+2} w_i \\ F_i w_0 = P''_i u_i + P''_{i+1} v_i + P''_{i+2} w_i \end{cases}$$

und

$$(27)\quad \begin{cases} \dfrac{u_i}{F_i} = p_i u_0 + p'_i v_0 + p''_i w_0 \\[2ex] \dfrac{v_i}{F_i} = q_i u_0 + q'_i v_0 + q''_i w_0 \\[2ex] \dfrac{w_i}{F_i} = r_i u_0 + r'_i v_0 + r''_i w_0 . \end{cases}$$

Die erste der Gleichungen (26) lehrt offenbar, dass F_i immer eine ganze complexe Zahl ist.

5. Nach diesen Vorbereitungen betrachten wir nun eine ganze complexe Zahl

$$x\alpha^2 + y\alpha + z$$

mit unbestimmten Coefficienten x, y, z. Ihre Norm $N(x, y, z)$, nämlich das Produkt

$$(28)\quad (x\alpha^2 + y\alpha + z)\cdot(x\beta^2 + y\beta + z)\cdot(x\gamma^2 + y\gamma + z)$$

ist offenbar eine homogene Funktion dritten Grades von x, y, z mit bezüglich der Wurzeln α, β, γ der kubischen Gleichung (19) symmetrischen also ganzzahligen Coefficienten, eine sogenannte ternäre kubische Form. Man findet sie in der That durch eine einfache Rechnung gleich

$$(29)\quad \begin{aligned} c_3^2 x^3 - c_2 c_3 x^2 y + c_1 c_3 x y^2 - c_3 y^3 + (c_2^2 - 2c_1 c_3) x^2 z \\ + (c_1^2 - 2c_2) x z^2 + c_2 y^2 z - c_1 y z^2 + (3c_3 - c_1 c_2) x y z + z^3. \end{aligned}$$

Wird nun auf diese Form die Substitution angewendet:

$$(30)\quad \begin{cases} x = P_i x' + P_{i+1} y' + P_{i+2} z' \\ y = P'_i x' + P'_{i+1} y' + P'_{i+2} z' \\ z = P''_i x' + P''_{i+1} y' + P''_{i+2} z', \end{cases}$$

so geht sie in eine andere ternäre kubische Form über, welche $N_i(x', y', z')$ heisse und durch den Ausdruck

$$
\begin{aligned}
&[p_i(\alpha)\cdot x' + p_{i+1}(\alpha)\cdot y' + p_{i+2}(\alpha)\cdot z']\\
&\cdot[p_i(\beta)\cdot x' + p_{i+1}(\beta)\cdot y' + p_{i+2}(\beta)\cdot z']\\
&\cdot[p_i(\gamma)\cdot x' + p_{i+1}(\gamma)\cdot y' + p_{i+2}(\gamma)\cdot z']
\end{aligned}
$$

gegeben wird, worin

$$
(31)\qquad p_i(\alpha) = P_i\alpha^2 + P_i'\alpha + P_i''
$$

und $p_i(\beta)$, $p_i(\gamma)$ die zu $p_i(\alpha)$ conjugirten complexen ganzen Zahlen sind, oder auch durch die Gleichung

$$
(32)\qquad N_i(x', y', z') = N_i(\alpha)\cdot N_i(\beta)\cdot N_i(\gamma),
$$

wenn gesetzt wird

$$
(33)\qquad \begin{cases}
N_i(\alpha) = p_i(\alpha)x' + p_{i+1}(\alpha)y' + p_{i+2}(\alpha)z'\\
N_i(\beta) = p_i(\beta)x' + p_{i+1}(\beta)y' + p_{i+2}(\beta)z'\\
N_i(\gamma) = p_i(\gamma)x' + p_{i+1}(\gamma)y' + p_{i+2}(\gamma)z'.
\end{cases}
$$

Werden aber zur Abkürzung die Bezeichnungen eingeführt:

$$
(34)\qquad \varpi_i = p_i(\alpha)p_i(\beta)p_i(\gamma),
$$

sodass ϖ_i eine positive ganze Zahl ist, und

$$
(35)\qquad \begin{cases}
\varphi_i(\alpha) = p_{i+1}(\alpha)p_i(\beta)p_i(\gamma)\\
\psi_i(\alpha) = p_{i+2}(\alpha)p_i(\beta)p_i(\gamma),
\end{cases}
$$

sodass $\varphi_i(\alpha)$, $\psi_i(\alpha)$ complexe ganze Zahlen sind, deren Werth gleichfalls positiv ist, und welche die Form haben:

$$
(36)\qquad \begin{cases}
\varphi_i(\alpha) = \xi_i'\alpha^2 + \eta_i'\alpha + \zeta_i'\\
\psi_i(\alpha) = \xi_i''\alpha^2 + \eta_i''\alpha + \zeta_i'',
\end{cases}
$$

so lassen sich die Gleichungen (33) auch in folgender Weise schreiben:

$$
(37)\qquad \begin{cases}
N_i(\alpha) = \dfrac{1}{p_i(\beta)\,p_i(\gamma)}\cdot[\varpi_i x' + \varphi_i(\alpha)\,y' + \psi_i(\alpha)\,z']\\[2ex]
N_i(\beta) = \dfrac{1}{p_i(\gamma)\,p_i(\alpha)}\cdot[\varpi_i x' + \varphi_i(\beta)\,y' + \psi_i(\beta)\,z']\\[2ex]
N_i(\gamma) = \dfrac{1}{p_i(\alpha)\,p_i(\beta)}\cdot[\varpi_i x' + \varphi_i(\gamma)\,y' + \psi_i(\gamma)\,z'].
\end{cases}
$$

Die Gleichungen (33) kann man entstanden denken durch Zusammensetzung der beiden Systeme linearer Gleichungen:

$$(38)\quad \begin{cases} N_i(\alpha) = x\alpha^2 + y\alpha + z \\ N_i(\beta) = x\beta^2 + y\beta + z \\ N_i(\gamma) = x\gamma^2 + y\gamma + z \end{cases}$$

und (30); demnach ist ihre Determinante gleich dem Produkte der Determinanten dieser Systeme, d. h. gleich der Discriminante der Gleichung (19) mal der Determinante (6), welche der Einheit gleich ist. Desgleichen können die Gleichungen (37) erhalten werden durch Zusammensetzung der Gleichungen

$$(39)\quad \begin{cases} N_i(\alpha) = \dfrac{1}{p_i(\beta)\,p_i(\gamma)} \cdot x_0 \\ N_i(\beta) = \dfrac{1}{p_i(\gamma)\,p_i(\alpha)} \cdot y_0 \\ N_i(\gamma) = \dfrac{1}{p_i(\alpha)\,p_i(\beta)} \cdot z_0 \end{cases}$$

zuerst mit den Gleichungen

$$(40)\quad \begin{cases} x_0 = x\alpha^2 + y\alpha + z \\ y_0 = x\beta^2 + y\beta + z \\ z_0 = x\gamma^2 + y\gamma + z \end{cases}$$

und darauf mit den Gleichungen

$$(41)\quad \begin{cases} x = \qquad\qquad \xi_i' y' + \xi_i'' z' \\ y = \qquad\qquad \eta_i' y' + \eta_i'' z' \\ z = \varpi_i x' + \zeta_i' y' + \zeta_i'' z'; \end{cases}$$

demnach ist ihre Determinante, d. h. die Determinante der gleichbedeutenden Gleichungen (33) auch gleich dem Produkte der Determinanten dieser drei Systeme (39), (40) und (41), und durch Vergleichung der so für die Determinante der Gleichungen (33) gefundenen beiden Werthe ergiebt sich ohne Weiteres die Beziehung:

$$1 = \frac{\varpi_i(\xi_i'\eta_i'' - \xi_i''\eta_i')}{p_i(\beta)\,p_i(\gamma)\cdot p_i(\gamma)\,p_i(\alpha)\cdot p_i(\alpha)\,p_i(\beta)}$$

oder einfacher die Gleichung:

$$(42)\quad \varpi_i = \xi_i'\eta_i'' - \xi_i''\eta_i'.$$

Die Formel (32) liefert, wenn man dem Index i alle möglichen Werthe beilegt, eine unbegrenzte Menge von

Formen, welche der Form $N(x, y, z)$ und daher auch unter einander äquivalent sind, da die Determinante der Substitutionen (30) der Einheit gleich ist. Um jede aus der vorhergehenden herzuleiten und so beliebig viele von ihnen allmählich zu berechnen, dient die Bemerkung, dass den Gleichungen (5) zufolge die Beziehung statthat:

$$p_{i+3}(\alpha) = p_i(\alpha) + l_i \cdot p_{i+1}(\alpha) + m_i \cdot p_{i+2}(\alpha).$$

Hiernach wird

$$(43) \qquad p_{i+1}(\alpha) x' + p_{i+2}(\alpha) y' + p_{i+3}(\alpha) z'$$
$$= p_i(\alpha) z' + p_{i+1}(\alpha)(x' + l_i z') + p_{i+2}(\alpha)(y' + m_i z')$$

d. h. $N_{i+1}(\alpha)$ geht aus $N_i(\alpha)$ hervor durch die Substitution

$$\begin{pmatrix} 0, & 0, & 1 \\ 1, & 0, & l_i \\ 0, & 1, & m_i \end{pmatrix}$$

und die solches aussprechende Gleichung (43) lässt sich schreiben wie folgt:

$$p_{i+1}(\beta) p_{i+1}(\gamma) \cdot \left[\varphi_i(\alpha) x' + \psi_i(\alpha) y' + \left(\varpi_i + l_i \varphi_i(\alpha) + m_i \psi_i(\alpha)\right) z'\right]$$
$$= p_i(\beta) p_i(\gamma) \cdot \left[\varpi_{i+1} x' + \varphi_{i+1}(\alpha) y' + \psi_{i+1}(\alpha) z'\right],$$

und ergiebt durch Vergleichung der Coefficienten von y', z' auf beiden Seiten folgende Formeln:

$$(44) \qquad \varphi_{i+1}(\alpha) = \frac{\varpi_{i+1} \cdot \psi_i(\alpha)}{\varphi_i(\alpha)}$$

$$(45) \qquad \psi_{i+1}(\alpha) = \frac{\varpi_{i+1}(\varpi_i + l_i \varphi_i(\alpha) + m_i \psi_i(\alpha))}{\varphi_i(\alpha)}.$$

Ferner findet man leicht bestätigt, dass

$$(46) \qquad N\varphi_i(\alpha) = \varpi_{i+1} \cdot \varpi_i^2$$

ist. Die Formeln (44), (45) und (46) dienen zur allmählichen Berechnung der Formen (32); in der That lässt sich vermittelst derselben aus der Form

$$N_i(x', y', z') = \frac{1}{\varpi_i^2} \cdot N\left(\varpi_i x' + \varphi_i(\alpha) y' + \psi_i(\alpha) z'\right)$$

unmittelbar die Form

$$N_{i+1}(x', y', z') = \frac{1}{\varpi_{i+1}^2} \cdot N(\varpi_{i+1} x' + \varphi_{i+1}(\alpha) y' + \psi_{i+1}(\alpha) z')$$

herleiten, sobald, wie angenommen wird, die Zahlen l_i, m_i bekannt sind.

6. Von nun an beschränken wir uns auf den Fall, dass die kubische Gleichung (19) die einfache Gestalt

$$x^3 - D = 0 \tag{47}$$

hat, während D eine positive ganze Zahl ist; so werden α, β, γ die drei Werthe der Kubikwurzel aus D, α ihr reeller Werth und folglich

$$\beta = \varrho\alpha, \quad \gamma = \varrho^2\alpha,$$

wo $\varrho^2 + \varrho + 1 = 0$ ist.

Aus den Gleichungen (26) ergiebt sich ohne Mühe

$$F_i p_i(\alpha) p_i(\gamma) \cdot (u_0\beta^2 + v_0\beta + w_0) = u_i \varpi_i + v_i \varphi_i(\beta) + w_i \psi_i(\beta).$$

Da aber $u_0 = 1$, $v_0 = \alpha$, $w_0 = \alpha^2$ gesetzt worden ist, wird

$$u_0\beta^2 + v_0\beta + w_0 = \varrho^2\alpha^2 + \varrho\alpha^2 + \alpha^2 = 0$$

sein, also kommt

$$u_i \varpi_i + v_i \varphi_i(\beta) + w_i \psi_i(\beta) = 0.$$

Hierin sind u_i, v_i, w_i reell; trennt man also das Reelle vom Imaginären, so entstehen folgende Gleichungen:

$$\begin{aligned} \varpi_i u_i + v_i \zeta_i' + w_i \zeta_i'' &= (v_i \eta_i' + w_i \eta_i'')\alpha \\ &= (v_i \xi_i' + w_i \xi_i'')\alpha^2 \end{aligned}$$

oder, anders geschrieben:

$$\frac{v_i}{u_i}(\eta_i'\alpha - \zeta_i') + \frac{w_i}{u_i}(\eta_i''\alpha - \zeta_i'') = \varpi_i$$

$$\frac{v_i}{u_i}(\xi_i'\alpha - \eta_i') + \frac{w_i}{u_i}(\xi_i''\alpha - \eta_i'') = 0.$$

Wir nennen $-\Delta_i$ die Determinante dieser Gleichungen und setzen

$$\begin{aligned} \varpi_i = \xi_i'\eta_i'' - \xi_i''\eta_i', \quad & \varpi_i' = \zeta_i'\xi_i'' - \zeta_i''\xi_i' \\ \varpi_i'' &= \eta_i'\zeta_i'' - \eta_i''\zeta_i', \end{aligned} \tag{48}$$

dann findet man

$$\Delta_i = \varpi_i\alpha^2 + \varpi_i'\alpha + \varpi_i'' \tag{49}$$

und durch Auflösung der Gleichungen nach $\frac{v_i}{u_i}$, $\frac{w_i}{u_i}$ folgende Werthe:

$$(50)\qquad \frac{v_i}{u_i} = -\frac{\varpi_i}{\Delta_i}(\xi_i''\alpha - \eta_i''), \quad \frac{w_i}{u_i} = \frac{\varpi_i}{\Delta_i}(\xi_i'\alpha - \eta_i').$$

Mit Hilfe dieser Gleichungen kann nun gezeigt werden, dass, wenn für zwei Werthe des Index i, etwa für $i = k$ und $i = k + h$, das Grössensystem

$$(51)\qquad \varpi_i,\ \varphi_i(\alpha),\ \psi_i(\alpha)$$

dieselben Werthe erhält, Gleiches auch von dem Grössensysteme

$$(52)\qquad \frac{v_i}{u_i},\ \frac{w_i}{u_i}$$

gelte und umgekehrt.

In der That, ist

$$(53)\quad \varpi_{k+h} = \varpi_k,\quad \varphi_{k+h}(\alpha) = \varphi_k(\alpha),\quad \psi_{k+h}(\alpha) = \psi_k(\alpha),$$

so wird $\varpi'_{k+h} = \varpi'_k$, $\varpi''_{k+h} = \varpi''_k$ sein müssen, und die Formeln (49) und (50) ergeben dann auch die Gleichungen:

$$(54)\qquad \frac{v_{k+h}}{u_{k+h}} = \frac{v_k}{u_k},\quad \frac{w_{k+h}}{u_{k+h}} = \frac{w_k}{u_k}.$$

Umgekehrt folgt aus den letzteren zunächst

$$\frac{w_{k+h}}{v_{k+h}} = \frac{w_k}{v_k}$$

oder nach (50):

$$\frac{\xi'_{k+h}\alpha - \eta'_{k+h}}{\xi''_{k+h}\alpha - \eta''_{k+h}} = \frac{\xi'_k\alpha - \eta'_k}{\xi''_k\alpha - \eta''_k}$$

d. h. die drei Gleichungen:

$$(55)\qquad \begin{gathered} \xi'_{k+h}\xi''_k - \xi''_{k+h}\xi'_k = 0, \quad \eta'_{k+h}\eta''_k - \eta''_{k+h}\eta'_k = 0 \\ \xi'_{k+h}\eta''_k - \eta''_{k+h}\xi'_k = \xi''_{k+h}\eta'_k - \eta'_{k+h}\xi''_k. \end{gathered}$$

Da

$$\varpi_k = \xi'_k\eta''_k - \xi''_k\eta'_k$$

nicht Null ist, muss eine der beiden Zahlen ξ'_k, ξ''_k wenigstens, etwa ξ''_k, von Null verschieden sein. Man findet also

$$\xi'_{k+h} = \frac{\xi'_k\xi''_{k+h}}{\xi''_k}.$$

Dann ist entweder: $\xi_k' = 0$ also $\xi_{k+h}' = 0$, aber η_k' nicht Null, folglich $\eta_{k+h}'' = \frac{\eta_{k+h}' \eta_k''}{\eta_k'}$. Ist nun erstens $\eta_k'' = 0$, so folgt $\eta_{k+h}'' = 0$ und die dritte der Gleichungen (55) giebt $\frac{\xi_{k+h}''}{\xi_k''} = \frac{\eta_{k+h}'}{\eta_k'}$, sodass man setzen kann:

$$(56) \qquad \begin{cases} \xi_{k+h}'' = z \cdot \xi_k'' & \eta_{k+h}' = z \cdot \eta_k' \\ \eta_{k+h}'' = z \cdot \eta_k'' & \xi_{k+h}' = z \cdot \xi_k', \end{cases}$$

während z eine gewisse rationale Zahl bedeutet. — Ist aber zweitens η_k'' nicht Null, so ergiebt sich

$$\frac{\eta_{k+h}''}{\eta_k''} = \frac{\eta_{k+h}'}{\eta_k'} = \frac{\xi_{k+h}''}{\xi_k''}$$

und daraus erhält man wieder dieselben Gleichungen (56).

Oder: ξ_k' ist nicht Null; dann kann nur eine der beiden Zahlen η_k', η_k'' Null sein, eine von ihnen, und es ist gleichgiltig, von welcher wir es voraussetzen, muss also von Null verschieden sein. Sei η_k' nicht Null, so folgt $\eta_{k+h}'' = \frac{\eta_{k+h}' \eta_k''}{\eta_k'}$. Ist jetzt erstens $\eta_k'' = 0$, so folgt auch $\eta_{k+h}'' = 0$ und

$$\frac{\eta_{k+h}'}{\eta_k'} = \frac{\xi_{k+h}''}{\xi_k''} = \frac{\xi_{k+h}'}{\xi_k'},$$

also wieder dieselben Gleichungen (56). — Wenn aber zweitens η_k'' nicht Null ist, so liefern die beiden ersten der Gleichungen (55)

$$\frac{\xi_{k+h}''}{\xi_k''} = \frac{\xi_{k+h}'}{\xi_k'}, \qquad \frac{\eta_{k+h}''}{\eta_k''} = \frac{\eta_{k+h}'}{\eta_k'},$$

die dritte aber kann geschrieben werden wie folgt:

$$\left(\frac{\eta_{k+h}''}{\eta_k''} - \frac{\xi_{k+h}'}{\xi_k'}\right) \cdot \left(\frac{\eta_k''}{\xi_k''} - \frac{\eta_k'}{\xi_k'}\right) = 0,$$

und liefert, da $\bar{\omega}_k$ und daher der zweite Faktor nicht Null ist, die Gleichheit $\frac{\xi_{k+h}'}{\xi_k'} = \frac{\eta_{k+h}''}{\eta_k''}$, also finden sich wiederum die Gleichungen (56).

Aus diesen ergiebt sich aber $\varpi_{k+h} = z^2 \cdot \varpi_k$, und, weil $\frac{v_{k+h}}{u_{k+h}} = \frac{v_k}{u_k}$ vorausgesetzt ist, $\varDelta_{k+h} = z^3 \cdot \varDelta_k$, d. h.

$$z^2 \varpi_k \cdot \alpha^2 + \varpi'_{k+h} \cdot \alpha + \varpi''_{k+h} = z^3 \varpi_k \cdot \alpha^2 + z^3 \varpi'_k \cdot \alpha + z^3 \varpi''_k,$$

woraus zuerst $z = 1$, also nach (56)

$$\xi''_{k+h} = \xi''_k, \quad \eta''_{k+h} = \eta''_k, \quad \xi'_{k+h} = \xi'_k, \quad \eta'_{k+h} = \eta'_k,$$

ferner

$$\varpi'_{k+h} = \varpi'_k, \quad \varpi''_{k+h} = \varpi''_k$$

oder

$$\xi''_k \cdot \zeta'_{k+h} - \xi'_k \cdot \zeta''_{k+h} = \xi''_k \cdot \zeta'_k - \xi'_k \cdot \zeta''_k$$

$$- \eta''_k \cdot \zeta'_{k+h} + \eta'_k \cdot \zeta''_{k+h} = - \eta''_k \cdot \zeta'_k + \eta'_k \cdot \zeta''_k,$$

also

$$\zeta'_{k+h} = \zeta'_k, \quad \zeta''_{k+h} = \zeta''_k,$$

und endlich, wie behauptet worden ist,

$$\varpi_{k+h} = \varpi_k, \quad \varphi_{k+h}(\alpha) = \varphi_k(\alpha), \quad \psi_{k+h}(\alpha) = \psi_k(\alpha)$$

gefunden wird.

7. Wenn nun aber die Gleichungen (53) oder (54) bestehen, so wird die Reihe der Grössensysteme (51) periodisch, indem von dem Systeme

$$\varpi_k, \quad \varphi_k(\alpha), \quad \psi_k(\alpha)$$

an eine Periode von h Gliedern unendlich oft sich wiederholen muss. Denn aus dem Bestehen der Gleichungen (53) und (54) folgt zunächst

$$l_{k+h} = l_k, \quad m_{k+h} = m_k,$$

sodann aber nach den Formeln (44), (45) und (46) auch

$$\varpi_{k+h+1} = \varpi_{k+1}, \quad \varphi_{k+h+1}(\alpha) = \varphi_{k+1}(\alpha), \quad \psi_{k+h+1}(\alpha) = \psi_{k+1}(\alpha)$$

u. s. f.

Diese Bemerkung, mit der vorigen verbunden, liefert den Satz: Wenn von den beiden Reihen von Grössensystemen (51) und (52) die eine periodisch ist, so hat die andere genau dieselbe Periode.

Die Periodicität der erstern Reihe tritt ein, sobald die Grössen (51) für ein unendlich wachsendes i endlich bleiben, und umgekehrt.

Das letztere ist offenbar. Um auch das erstere zu zeigen, nehmen wir an, es sei für jedes i

$$\bar{\omega}_i < A, \quad \varphi_i(\alpha) < B, \quad \psi_i(\alpha) < C,$$

während A, B, C endliche Constanten sind. Setzt man dann

$$\varphi_i(\beta) = re^{s\sqrt{-1}}, \quad \varphi_i(\gamma) = re^{-s\sqrt{-1}},$$

wo $r > 0$ sei, so ist

$$r^2 = \varphi_i(\beta)\varphi_i(\gamma) = \frac{p_i(\alpha)}{p_{i+1}(\alpha)} \cdot \bar{\omega}_i \bar{\omega}_{i+1}$$

also, da nach den Gleichungen (5) die Grössen P_i, P_i', P_i'' und deshalb nach der Definitionsgleichung (31) auch $p_i(\alpha)$ mit wachsendem i immer grösser werden,

$$r^2 < \bar{\omega}_i \bar{\omega}_{i+1} < A^2, \quad r < A.$$

Daher kann man setzen:

$$\varphi_i(\alpha) = \xi_i'\alpha^2 + \eta_i'\alpha + \zeta_i' = \varepsilon B$$
$$\varphi_i(\beta) = \xi_i'\beta^2 + \eta_i'\beta + \zeta_i' = \varepsilon' A(\cos s + \sqrt{-1}\cdot\sin s)$$
$$\varphi_i(\gamma) = \xi_i'\gamma^2 + \eta_i'\gamma + \zeta_i' = \varepsilon' A(\cos s - \sqrt{-1}\cdot\sin s),$$

woraus sich

$$3\zeta_i' = \varepsilon B + 2\varepsilon' A\cdot\cos s$$
$$3\alpha\eta_i' = \varepsilon B + 2\varepsilon' A\cdot\cos\left(s - \frac{2\pi}{3}\right)$$
$$3\alpha^2\xi_i' = \varepsilon B + 2\varepsilon' A\cdot\cos\left(s + \frac{2\pi}{3}\right)$$

ergeben, während ε, ε' positive echte Brüche bedeuten. Aehnliches gilt von ξ_i'', η_i'', ζ_i''. Da demnach diese ganzen Zahlen nur eine endliche Anzahl verschiedener Werthe erhalten können, müssen zwei der Grössensysteme (51) einander gleich werden, und Periodicität in der Reihe derselben eintreten.

8. Suchen wir nun die Bedingung dafür, dass $\bar{\omega}_i$, $\varphi_i(\alpha)$, $\psi_i(\alpha)$ endlich bleiben, wenn i über jede Grenze hinaus wächst. Man findet leicht die Formel:

$$u_i p_i(\alpha) + v_i p_{i+1}(\alpha) + w_i p_{i+2}(\alpha) = 3\alpha^2\cdot F_i,$$

welche man auch so schreiben kann:

$$\bar{\omega}_i + \frac{v_i}{u_i}\varphi_i(\alpha) + \frac{w_i}{u_i}\psi_i(\alpha) = 3\alpha^2\cdot\frac{F_i}{u_i}p_i(\beta)p_i(\gamma). \tag{57}$$

Hieraus ergiebt sich, indem man für $\frac{v_i}{u_i}$, $\frac{w_i}{u_i}$ die unter (50) angegebenen Werthe einsetzt und die Gleichung

$$(58)\quad (\xi_i'\alpha - \eta_i')\psi_i(\alpha) - (\xi_i''\alpha - \eta_i'')\varphi_i(\alpha) = 3\varpi_i\alpha^2 - \Delta_i$$

beachtet, für Δ_i folgender positive Werth:

$$(59)\qquad \Delta_i = \varpi_i \cdot \frac{u_i}{F_i}\, p_i(\alpha)$$

und damit und mit Rücksicht darauf, dass auch $\frac{v_i}{u_i}$, $\frac{w_i}{u_i}$ in den Formeln (50) positiv sind, aus der Gleichung (58) die Ungleichheit:

$$(60)\qquad \Delta_i < 3\varpi_i \cdot \alpha^2.$$

Hiernach ist $\frac{\Delta_i}{\varpi_i}$ d. h. (nach (59)) $\frac{u_i}{F_i}\, p_i(\alpha)$ stets kleiner als $3\alpha^2$, bleibt also bei unendlich wachsendem Index i endlich; es kann aber auch dabei nicht unendlich klein werden, sobald ϖ_i, $\varphi_i(\alpha)$, $\psi_i(\alpha)$ endlich bleiben. Denn alsdann erhalten ϖ_i und, wie wir gesehen haben, auch ξ_i', η_i', ζ_i', ξ_i'', η_i'', ζ_i'' und folglich auch $\frac{\Delta_i}{\varpi_i}$ nur eine endliche Anzahl von Werthen, nicht eine unbegrenzte Reihe von Werthen, welche gegen Null convergirt. Weil nun

$$\varpi_i = \frac{u_i}{F_i}\, p_i(\alpha) \cdot \frac{F_i}{u_i}\, p_i(\beta)\, p_i(\gamma)$$

gesetzt werden kann, folgt aus dem eben Gesagten, dass, wenn ϖ_i, $\varphi_i(\alpha)$, $\psi_i(\alpha)$ bei wachsendem i unter einer endlichen Grenze bleiben sollen, nothwendigerweise $\frac{F_i}{u_i}\, p_i(\beta)\, p_i(\gamma)$ gleichfalls endlich bleiben muss.

Diese nothwendige Bedingung ist aber auch hinreichend. Hierzu bemerken wir zuerst, dass die erste und letzte der Gleichungen (25), wenn zugleich i um eine Einheit verringert wird, durch Division mit einander folgende neue Gleichung geben:

$$\frac{w_i}{u_i} = \frac{1}{\frac{v_{i-1}}{u_{i-1}} - l_{i-1}};$$

ihr zufolge ist $\frac{w_i}{u_i}$ stets grösser als Eins. Ferner ist

$$\varphi_i(\alpha) = p_{i+1}(\alpha) \cdot p_i(\beta)\, p_i(\gamma)$$

kleiner als

$$\psi_i(\alpha) = p_{i+2}(\alpha) \cdot p_i(\beta) p_i(\gamma),$$

da $p_{i+1}(\alpha) < p_{i+2}(\alpha)$ ist. Demgemäss folgt aus der Gleichung (57) sofort:

$$\varpi_i < 3\alpha^2 \cdot \frac{F_i}{u_i} p_i(\beta) p_i(\gamma)$$

$$\psi_i(\alpha) < 3\alpha^2 \cdot \frac{F_i}{u_i} p_i(\beta) p_i(\gamma)$$

$$\varphi_i(\alpha) < 3\alpha^2 \cdot \frac{F_i}{u_i} p_i(\beta) p_i(\gamma),$$

und daher bleiben in der That ϖ_i, $\varphi_i(\alpha)$, $\psi_i(\alpha)$ endlich zugleich mit $\frac{F_i}{u_i} p_i(\beta) p_i(\gamma)$. So wird der Satz erhalten:

Damit die Reihe der Grössensysteme (51) oder (52) periodisch werde, ist nothwendig und hinreichend, dass $\frac{F_i}{u_i} p_i(\beta) p_i(\gamma)$ endlich bleibt, während i über jede Grenze hinaus wächst.

Man kann demselben leicht eine andere Form geben. Denn man bestätigt ohne Mühe folgende Gleichheit:

$$2p_i(\beta) p_i(\gamma) = (P_i'' - P_i'\alpha)^2 + (P_i'' - P_i\alpha^2)^2 + \alpha^2 \cdot (P_i' - P_i\alpha)^2.$$

Soll demnach $\frac{F_i}{u_i} p_i(\beta) p_i(\gamma)$ endlich bleiben, so müssen auch die beiden Ausdrücke

$$(P_i'' - P_i\alpha^2)\sqrt{\frac{F_i}{u_i}}, \quad (P_i' - P_i\alpha)\sqrt{\frac{F_i}{u_i}}$$

endlich bleiben; umgekehrt, wenn diese endlich bleiben, so gilt dasselbe auch von $(P_i'' - P_i'\alpha)\sqrt{\frac{F_i}{u_i}}$ und folglich auch von $\frac{F_i}{u_i} p_i(\beta) p_i(\gamma)$. — Aus der ersten der Gleichungen (26) folgt noch $\frac{P_i u_i}{F_i} < 1$.

Diese Bemerkungen reichen hin, um den vorigen Satz auch folgendermassen fassen zu können:

Zur Periodicität der Reihen von Grössensystemen (51) und (52) ist nothwendig und hinreichend, dass die Ungleichheit

$$(57)\quad (P_i' - P_i\alpha)^2 + (P_i'' - P_i\alpha^2)^2 + \left(\frac{u_i}{F_i}\right)^3 \cdot P_i^2 < k \cdot \frac{u_i}{F_i}$$

für alle Werthe von i erfüllt sei, während k eine passend gewählte endliche Constante bezeichnet.

Diese neue Fassung zeigt auf's Deutlichste an, dass zwischen den aus dem Jacobi'schen Kettenbruchalgorithmus entspringenden ganzen Zahlen P_i, P_i', P_i'' einerseits und denjenigen andern ganzen Zahlen X, Y, Z, für welche die Ausdrücke $Y - \alpha X$, $Z - \alpha^2 X$ gleichzeitige Minima werden, oder für welche die quadratische Form

$$f = (Y - \alpha X)^2 + (Z - \alpha^2 X)^2 + \frac{X^2}{\varDelta},$$

entsprechend den veränderlichen Werthen von $\varDelta$, ihre aufeinanderfolgenden Minima annimmt — Aufgaben, wie Hermite sie in seinen zahlentheoretischen Briefen zu lösen unternimmt — ein naher Zusammenhang bestehen muss; man vergleiche in dieser Hinsicht nur die Stellen jener Briefe, welche sich finden a. a. O. pag. 265 und 295. Auch lehrt jener Satz (57) das Gesetz kennen, nach welchem die Näherungsbrüche $\frac{P_i'}{P_i}$, $\frac{P_i''}{P_i}$ mit gleichem Nenner den Werthen α, α^2 resp. sich annähern, *so oft* der Kettenbruchalgorithmus periodisch wird. Denn da in diesem Falle die Ungleichheit (57) besteht, ergeben sich daraus leicht auch die nachstehenden:

$$\frac{P_i'}{P_i} - \alpha < \frac{k^{\frac{1}{2}}}{P_i\sqrt{P_i}}, \quad \frac{P_i''}{P_i} - \alpha^2 < \frac{k^{\frac{1}{2}}}{P_i\sqrt{P_i}},$$

welche das Annäherungsgesetz aussprechen. — Wie sich nun aber jener erwähnte Zusammenhang gestalte und ob der Kettenbruchalgorithmus allzeit periodisch sei, bleibt noch eine offene Frage.

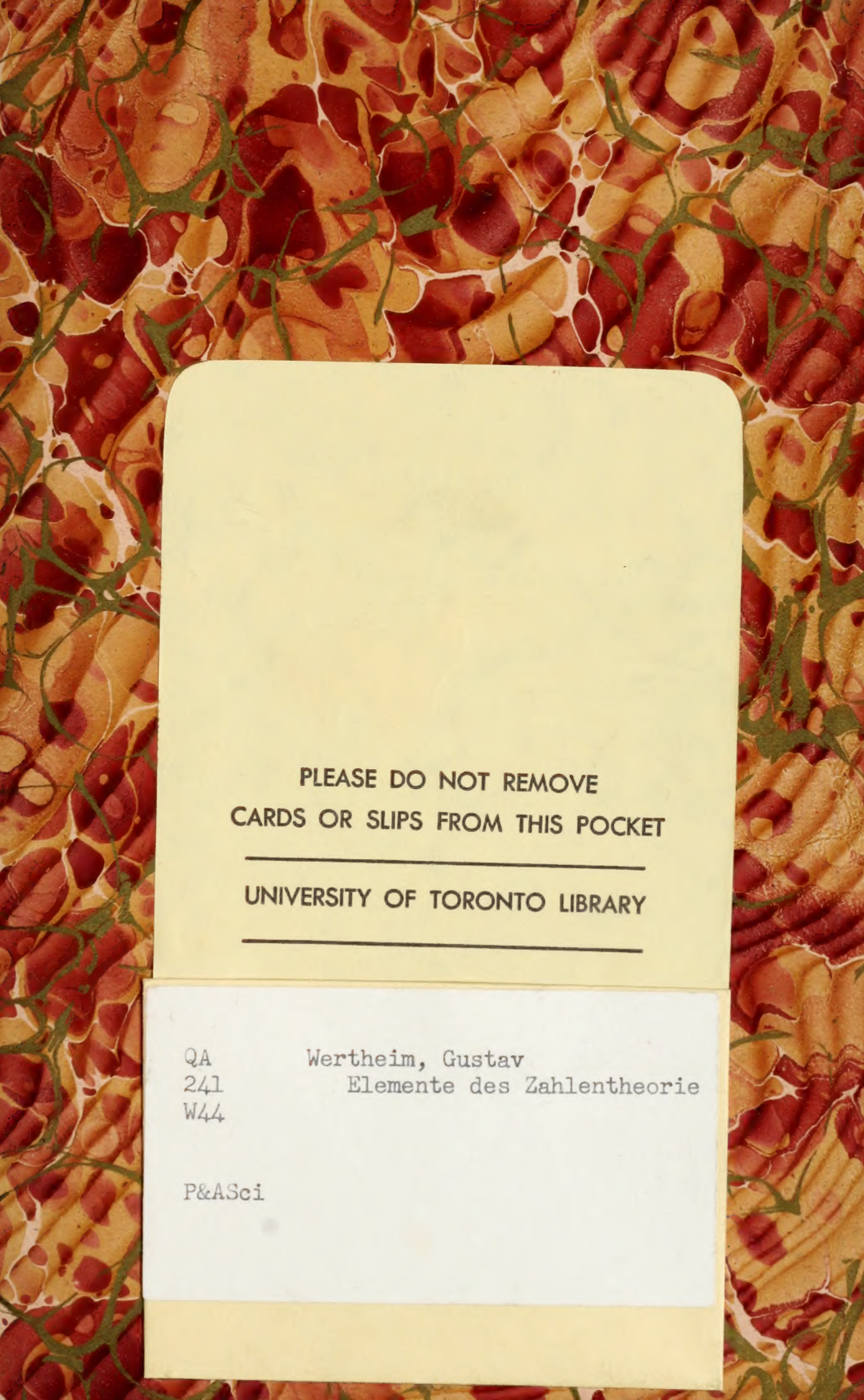











PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET
UNIVERSITY OF TORONTO LIBRARY
QA
241
W44
Wertheim, Gustav
Elemente des Zahlentheorie
P&ASci

